Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Acer					
quick_access					
Untrusted Search Path	17-12-2019	6.9	In the Quick Access Service (QAAdminAgent.exe) in Acer Quick Access V2.01.3000 through 2.01.3027 and V3.00.3000 through V3.00.3008, a REGULAR user can load an arbitrary unsigned DLL into the signed service's process, which is running as NT AUTHORITY\SYSTEM. This is a DLL Hijacking vulnerability (including search order hijacking, which searches for the missing DLL in the PATH environment variable), which is caused by an uncontrolled search path element for nvapi.dll, atiadlxx.dll, or atiadlxy.dll. **CVE ID : CVE-2019-18670**	https://us.answers.acer.com/app/answers/detail/a_id/64586	A-ACE-QUIC-060120/1
Adobe					
acrobat_dc					
Improper Privilege Management	19-12-2019	7.5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have a binary planting (default folder privilege escalation) vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2019-16444**		
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16445**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/3
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16446**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/4
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/5

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16448**		
Information Exposure	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16449**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/6
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16450**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/7
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a heap overflow	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16451**		
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16452**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/9
Improper Input Validation	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a security bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-16453**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/10
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds write vulnerability. Successful exploitation could	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution . **CVE ID : CVE-2019-16454**		
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16455**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/12
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16456**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/13
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to information disclosure . **CVE ID : CVE-2019-16457**		
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16458**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/15
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16459**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/16
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution . **CVE ID : CVE-2019-16460**		
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16461**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/18
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16462**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/19
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16463		
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16464**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/21
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16465**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/22
acrobat_reader_dc					
Improper Privilege Management	19-12-2019	7.5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a binary planting (default folder privilege escalation) vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege escalation. **CVE ID : CVE-2019-16444**		
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16445**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/24
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16446**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/25
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16448**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/26

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16449**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/27
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16450**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/28
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16451**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/29
Use After	19-12-2019	10	Adobe Acrobat and Reader	https://hel	A-ADO-ACRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16452**	px.adobe.com/security/products/acrobat/apsb19-55.html	060120/30
Improper Input Validation	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a security bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-16453**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/31
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16454**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/32
NULL Pointer	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056	https://helpx.adobe.co	A-ADO-ACRO-060120/33

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16455**	m/security /products/ acrobat/aps b19-55.html	
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16456**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/34
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16457**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/35
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056	https://helpx.adobe.co	A-ADO-ACRO-060120/36

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16458**	m/security /products/ acrobat/apsb19-55.html	
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16459**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/37
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16460**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/38
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152	https://helpx.adobe.com/security	A-ADO-ACRO-060120/39

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16461**	/products/acrobat/apsb19-55.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16462**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/40
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16463**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/41
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155	https://helpx.adobe.com/security/products/	A-ADO-ACRO-060120/42

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16464**	acrobat/apsb19-55.html	
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16465**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	A-ADO-ACRO-060120/43
coldfusion					
Incorrect Default Permissions	19-12-2019	7.5	ColdFusion versions Update 6 and earlier have an insecure inherited permissions of default installation directory vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2019-8256**	https://helpx.adobe.com/security/products/coldfusion/apsb19-58.html	A-ADO-COLD-060120/44
photoshop_cc					
Improper Restriction of Operations within the Bounds of a Memory	19-12-2019	9.3	Adobe Photoshop CC versions before 20.0.8 and 21.0.x before 21.0.2 have a memory corruption vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/photoshop/apsb19-	A-ADO-PHOT-060120/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			arbitrary code execution. **CVE ID : CVE-2019-8253**	56.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-12-2019	9.3	Adobe Photoshop CC versions before 20.0.8 and 21.0.x before 21.0.2 have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8254**	https://helpx.adobe.com/security/products/photoshop/apsb19-56.html	A-ADO-PHOT-060120/46
brackets					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-12-2019	10	Brackets versions 1.14 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8255**	https://helpx.adobe.com/security/products/brackets/apsb19-57.html	A-ADO-BRAC-060120/47
Altn					
mdaemon_email_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-12-2019	3.5	MDaemon Email Server 17.5.1 allows XSS via the filename of an attachment to an email message. **CVE ID : CVE-2019-19497**	N/A	A-ALT-MDAE-060120/48
Apache					
incubator_superset					
Information Exposure	16-12-2019	5	In Apache Incubator Superset before 0.31 user could query database metadata information from a database he has no access to, by using a specially crafted	N/A	A-APA-INCU-060120/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			complex query. **CVE ID : CVE-2019-12413**		
Information Exposure	16-12-2019	5	In Apache Incubator Superset before 0.32, a user can view database names that he has no access to on a dropdown list in SQLLab **CVE ID : CVE-2019-12414**	N/A	A-APA-INCU-060120/50
Apple					
xcode					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in Xcode 11.0. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2019-8739**	N/A	A-APP-XCOD-060120/51
Improper Input Validation	18-12-2019	9.3	Multiple issues in ld64 in the Xcode toolchains were addressed by updating to version ld64-507.4. This issue is fixed in Xcode 11.0. Compiling code without proper input validation could lead to arbitrary code execution with user privilege. **CVE ID : CVE-2019-8721**	N/A	A-APP-XCOD-060120/52
Improper Input Validation	18-12-2019	9.3	Multiple issues in ld64 in the Xcode toolchains were addressed by updating to version ld64-507.4. This issue is fixed in Xcode 11.0. Compiling code without proper input validation could lead to arbitrary code	N/A	A-APP-XCOD-060120/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution with user privilege. **CVE ID : CVE-2019-8722**		
Improper Input Validation	18-12-2019	9.3	Multiple issues in ld64 in the Xcode toolchains were addressed by updating to version ld64-507.4. This issue is fixed in Xcode 11.0. Compiling code without proper input validation could lead to arbitrary code execution with user privilege. **CVE ID : CVE-2019-8723**	N/A	A-APP-XCOD-060120/54
Improper Input Validation	18-12-2019	9.3	Multiple issues in ld64 in the Xcode toolchains were addressed by updating to version ld64-507.4. This issue is fixed in Xcode 11.0. Compiling code without proper input validation could lead to arbitrary code execution with user privilege. **CVE ID : CVE-2019-8724**	N/A	A-APP-XCOD-060120/55
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in Xcode 11.0. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2019-8738**	N/A	A-APP-XCOD-060120/56
Improper Restriction of Operations within the	18-12-2019	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in Xcode 11.2. Processing a maliciously	N/A	A-APP-XCOD-060120/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			crafted file may lead to arbitrary code execution. **CVE ID : CVE-2019-8800**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in Xcode 11.2. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2019-8806**	N/A	A-APP-XCOD-060120/58
icloud					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15, tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2019-8745**	N/A	A-APP-ICLO-060120/59
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in watchOS 6.1, iCloud for Windows 11.0. Multiple issues in libxslt. **CVE ID : CVE-2019-8750**	N/A	A-APP-ICLO-060120/60
Improper Restriction of Operations within the Bounds of a	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.1 and iPadOS 13.1, tvOS 13, Safari 13.0.1, iTunes for	N/A	A-APP-ICLO-060120/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8763**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8766**	N/A	A-APP-ICLO-060120/62
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8782**	N/A	A-APP-ICLO-060120/63
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web	N/A	A-APP-ICLO-060120/64

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			content may lead to arbitrary code execution. **CVE ID : CVE-2019-8783**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8784**	N/A	A-APP-ICLO-060120/65
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-12-2019	7.6	A race condition existed during the installation of iTunes for Windows. This was addressed with improved state handling. This issue is fixed in iCloud for Windows 7.11. Running the iTunes installer in an untrusted directory may result in arbitrary code execution. **CVE ID : CVE-2019-6232**	N/A	A-APP-ICLO-060120/66
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-12-2019	7.6	A race condition existed during the installation of iCloud for Windows. This was addressed with improved state handling. This issue is fixed in iCloud for Windows 7.11. Running the iCloud installer in an untrusted directory may result in arbitrary code execution.	N/A	A-APP-ICLO-060120/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6236		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8523**	N/A	A-APP-ICLO-060120/68
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8535**	N/A	A-APP-ICLO-060120/69
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8536**	N/A	A-APP-ICLO-060120/70
Buffer Copy without	18-12-2019	6.8	A buffer overflow was addressed with improved	N/A	A-APP-ICLO-060120/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			bounds checking. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8544**	N/A	A-APP-ICLO-060120/72
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8551**	N/A	A-APP-ICLO-060120/73
Use After Free	18-12-2019	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11.	N/A	A-APP-ICLO-060120/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8556**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8558**	N/A	A-APP-ICLO-060120/75
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8559**	N/A	A-APP-ICLO-060120/76
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to	N/A	A-APP-ICLO-060120/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2019-8563**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8571**	N/A	A-APP-ICLO-060120/78
Improper Input Validation	18-12-2019	6.8	An input validation issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8577**	N/A	A-APP-ICLO-060120/79
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8583**	N/A	A-APP-ICLO-060120/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8584**	N/A	A-APP-ICLO-060120/81
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8586**	N/A	A-APP-ICLO-060120/82
Improper Validation of Array Index	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8587**	N/A	A-APP-ICLO-060120/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8594**	N/A	A-APP-ICLO-060120/84
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8595**	N/A	A-APP-ICLO-060120/85
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8596**	N/A	A-APP-ICLO-060120/86

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8597**	N/A	A-APP-ICLO-060120/87
Improper Input Validation	18-12-2019	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to read restricted memory. **CVE ID : CVE-2019-8598**	N/A	A-APP-ICLO-060120/88
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A maliciously crafted SQL query may lead to arbitrary code execution. **CVE ID : CVE-2019-8600**	N/A	A-APP-ICLO-060120/89
Integer Overflow or	18-12-2019	6.8	Multiple memory corruption issues were addressed with	N/A	A-APP-ICLO-060120/90

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8601**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8602**	N/A	A-APP-ICLO-060120/91
Out-of-bounds Read	18-12-2019	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may result in the disclosure of process memory. **CVE ID : CVE-2019-8607**	N/A	A-APP-ICLO-060120/92
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS	N/A	A-APP-ICLO-060120/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8608**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8609**	N/A	A-APP-ICLO-060120/94
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8610**	N/A	A-APP-ICLO-060120/95
Improper Restriction of Operations	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS	N/A	A-APP-ICLO-060120/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8611**		
Out-of-bounds Read	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8615**	N/A	A-APP-ICLO-060120/97
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8619**	N/A	A-APP-ICLO-060120/98
Improper Restriction of Operations	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS	N/A	A-APP-ICLO-060120/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8622**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8623**	N/A	A-APP-ICLO-060120/100
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8625**	N/A	A-APP-ICLO-060120/101
Improper Restriction of Operations within the Bounds of a	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1,	N/A	A-APP-ICLO-060120/102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8628**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8644**	N/A	A-APP-ICLO-060120/103
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of synchronous page loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8649**	N/A	A-APP-ICLO-060120/104
Out-of-bounds Read	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is	N/A	A-APP-ICLO-060120/105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8658**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8666**	N/A	A-APP-ICLO-060120/106
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8669**	N/A	A-APP-ICLO-060120/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8671**	N/A	A-APP-ICLO-060120/108
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8672**	N/A	A-APP-ICLO-060120/109
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code	N/A	A-APP-ICLO-060120/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2019-8673**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8676**	N/A	A-APP-ICLO-060120/111
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8677**	N/A	A-APP-ICLO-060120/112
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6.	N/A	A-APP-ICLO-060120/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8678**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8679**	N/A	A-APP-ICLO-060120/114
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8680**	N/A	A-APP-ICLO-060120/115
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2,	N/A	A-APP-ICLO-060120/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8681**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8683**	N/A	A-APP-ICLO-060120/117
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8684**	N/A	A-APP-ICLO-060120/118
Improper Restriction of	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling.	N/A	A-APP-ICLO-060120/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8685**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8686**	N/A	A-APP-ICLO-060120/120
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8687**	N/A	A-APP-ICLO-060120/121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8688**	N/A	A-APP-ICLO-060120/122
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8689**	N/A	A-APP-ICLO-060120/123
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of document loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web	N/A	A-APP-ICLO-060120/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			content may lead to universal cross site scripting. **CVE ID : CVE-2019-8690**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8707**	N/A	A-APP-ICLO-060120/125
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8710**	N/A	A-APP-ICLO-060120/126
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8719**	N/A	A-APP-ICLO-060120/127
Improper Restriction of	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling.	N/A	A-APP-ICLO-060120/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8726**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8733**	N/A	A-APP-ICLO-060120/129
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8735**	N/A	A-APP-ICLO-060120/130
Improper Restriction of Operations within the Bounds of a	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3,	N/A	A-APP-ICLO-060120/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8811**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8813**	N/A	A-APP-ICLO-060120/132
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8814**	N/A	A-APP-ICLO-060120/133
Improper Restriction of Operations within the Bounds of a	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for	N/A	A-APP-ICLO-060120/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8815**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8816**	N/A	A-APP-ICLO-060120/135
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8819**	N/A	A-APP-ICLO-060120/136
Improper Restriction of Operations within the	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2,	N/A	A-APP-ICLO-060120/137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8820**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8821**	N/A	A-APP-ICLO-060120/138
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8822**	N/A	A-APP-ICLO-060120/139
Improper Restriction of Operations	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2	N/A	A-APP-ICLO-060120/140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8823**		
itunes					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15, tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2019-8745**	N/A	A-APP-ITUN-060120/141
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.1 and iPadOS 13.1, tvOS 13, Safari 13.0.1, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8763**	N/A	A-APP-ITUN-060120/142
Improper Restriction of Operations	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2	N/A	A-APP-ITUN-060120/143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8782**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8783**	N/A	A-APP-ITUN-060120/144
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8784**	N/A	A-APP-ITUN-060120/145
Improper Restriction of Operations within the	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1,	N/A	A-APP-ITUN-060120/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8523**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8535**	N/A	A-APP-ITUN-060120/147
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8536**	N/A	A-APP-ITUN-060120/148
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. A malicious	N/A	A-APP-ITUN-060120/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application may be able to elevate privileges. **CVE ID : CVE-2019-8542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8544**	N/A	A-APP-ITUN-060120/150
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8551**	N/A	A-APP-ITUN-060120/151
Use After Free	18-12-2019	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8556**	N/A	A-APP-ITUN-060120/152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8558**	N/A	A-APP-ITUN-060120/153
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8559**	N/A	A-APP-ITUN-060120/154
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2019-8562**	N/A	A-APP-ITUN-060120/155
Improper Restriction of Operations within the	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2,	N/A	A-APP-ITUN-060120/156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8563**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8571**	N/A	A-APP-ITUN-060120/157
Improper Input Validation	18-12-2019	6.8	An input validation issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8577**	N/A	A-APP-ITUN-060120/158
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for	N/A	A-APP-ITUN-060120/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8583**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8584**	N/A	A-APP-ITUN-060120/160
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8586**	N/A	A-APP-ITUN-060120/161
Improper Validation of Array Index	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12.	N/A	A-APP-ITUN-060120/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8587**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8594**	N/A	A-APP-ITUN-060120/163
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8595**	N/A	A-APP-ITUN-060120/164
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12.	N/A	A-APP-ITUN-060120/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8596**		
Access of Resource Using Incompatible Type ('Type Confusion')	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8597**	N/A	A-APP-ITUN-060120/166
Improper Input Validation	18-12-2019	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to read restricted memory. **CVE ID : CVE-2019-8598**	N/A	A-APP-ITUN-060120/167
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A maliciously crafted SQL	N/A	A-APP-ITUN-060120/168

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			query may lead to arbitrary code execution. **CVE ID : CVE-2019-8600**		
Integer Overflow or Wraparound	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8601**	N/A	A-APP-ITUN-060120/169
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8602**	N/A	A-APP-ITUN-060120/170
Out-of-bounds Read	18-12-2019	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may result in the disclosure of process memory.	N/A	A-APP-ITUN-060120/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8607		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8608**	N/A	A-APP-ITUN-060120/172
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8609**	N/A	A-APP-ITUN-060120/173
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	A-APP-ITUN-060120/174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8610		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8611**	N/A	A-APP-ITUN-060120/175
Out-of-bounds Read	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8615**	N/A	A-APP-ITUN-060120/176
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	A-APP-ITUN-060120/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8619		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8622**	N/A	A-APP-ITUN-060120/178
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8623**	N/A	A-APP-ITUN-060120/179
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8625**	N/A	A-APP-ITUN-060120/180
Improper	18-12-2019	6.8	Multiple memory corruption	N/A	A-APP-ITUN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8628**		060120/181
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8644**	N/A	A-APP-ITUN-060120/182
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of synchronous page loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting.	N/A	A-APP-ITUN-060120/183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8649		
Out-of-bounds Read	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8658**	N/A	A-APP-ITUN-060120/184
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8666**	N/A	A-APP-ITUN-060120/185
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web	N/A	A-APP-ITUN-060120/186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			content may lead to arbitrary code execution. **CVE ID : CVE-2019-8669**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8671**	N/A	A-APP-ITUN-060120/187
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8672**	N/A	A-APP-ITUN-060120/188
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13,	N/A	A-APP-ITUN-060120/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8673**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8676**	N/A	A-APP-ITUN-060120/190
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8677**	N/A	A-APP-ITUN-060120/191
Improper Restriction of Operations within the	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6,	N/A	A-APP-ITUN-060120/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8678**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8679**	N/A	A-APP-ITUN-060120/193
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8680**	N/A	A-APP-ITUN-060120/194
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with	N/A	A-APP-ITUN-060120/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8681**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8683**	N/A	A-APP-ITUN-060120/196
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	A-APP-ITUN-060120/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8684		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8685**	N/A	A-APP-ITUN-060120/198
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8686**	N/A	A-APP-ITUN-060120/199
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may	N/A	A-APP-ITUN-060120/200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2019-8687**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8688**	N/A	A-APP-ITUN-060120/201
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8689**	N/A	A-APP-ITUN-060120/202
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of document loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for	N/A	A-APP-ITUN-060120/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8690**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8707**	N/A	A-APP-ITUN-060120/204
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8719**	N/A	A-APP-ITUN-060120/205
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may	N/A	A-APP-ITUN-060120/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2019-8726**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8733**	N/A	A-APP-ITUN-060120/207
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8735**	N/A	A-APP-ITUN-060120/208
Untrusted Search Path	18-12-2019	4.4	A dynamic library loading issue existed in iTunes setup. This was addressed with improved path searching. This issue is fixed in macOS Catalina 10.15.1, iTunes for Windows 12.10.2. Running the iTunes installer in an untrusted directory may result in arbitrary code execution. **CVE ID : CVE-2019-8801**	N/A	A-APP-ITUN-060120/209

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8808**	N/A	A-APP-ITUN-060120/210
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8811**	N/A	A-APP-ITUN-060120/211
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8812**	N/A	A-APP-ITUN-060120/212
Improper	18-12-2019	4.3	A logic issue was addressed	N/A	A-APP-ITUN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8813**		060120/213
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8814**	N/A	A-APP-ITUN-060120/214
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8815**	N/A	A-APP-ITUN-060120/215
Improper Restriction	18-12-2019	9.3	Multiple memory corruption issues were addressed with	N/A	A-APP-ITUN-060120/216

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8816**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8819**	N/A	A-APP-ITUN-060120/217
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8820**	N/A	A-APP-ITUN-060120/218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8821**	N/A	A-APP-ITUN-060120/219
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8822**	N/A	A-APP-ITUN-060120/220
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8823**	N/A	A-APP-ITUN-060120/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
safari					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.1 and iPadOS 13.1, tvOS 13, Safari 13.0.1, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8763**	N/A	A-APP-SAFA-060120/222
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8782**	N/A	A-APP-SAFA-060120/223
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8783**	N/A	A-APP-SAFA-060120/224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8523**	N/A	A-APP-SAFA-060120/225
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8535**	N/A	A-APP-SAFA-060120/226
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8536**	N/A	A-APP-SAFA-060120/227
Improper Restriction of	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling.	N/A	A-APP-SAFA-060120/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8544**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8551**	N/A	A-APP-SAFA-060120/229
Use After Free	18-12-2019	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8556**	N/A	A-APP-SAFA-060120/230
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for	N/A	A-APP-SAFA-060120/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8558**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8559**	N/A	A-APP-SAFA-060120/232
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2019-8562**	N/A	A-APP-SAFA-060120/233
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8563**	N/A	A-APP-SAFA-060120/234

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8571**	N/A	A-APP-SAFA-060120/235
Improper Input Validation	18-12-2019	6.8	An input validation issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8577**	N/A	A-APP-SAFA-060120/236
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8583**	N/A	A-APP-SAFA-060120/237
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with	N/A	A-APP-SAFA-060120/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8584**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8586**	N/A	A-APP-SAFA-060120/239
Improper Validation of Array Index	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8587**	N/A	A-APP-SAFA-060120/240
Improper Restriction	18-12-2019	6.8	Multiple memory corruption issues were addressed with	N/A	A-APP-SAFA-060120/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8594**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8595**	N/A	A-APP-SAFA-060120/242
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8596**	N/A	A-APP-SAFA-060120/243
Access of Resource	18-12-2019	4.3	Multiple memory corruption issues were addressed with	N/A	A-APP-SAFA-060120/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Using Incompatible Type ('Type Confusion')			improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8597**		
Integer Overflow or Wraparound	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8601**	N/A	A-APP-SAFA-060120/245
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8602**	N/A	A-APP-SAFA-060120/246
Out-of-bounds Read	18-12-2019	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS	N/A	A-APP-SAFA-060120/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may result in the disclosure of process memory. **CVE ID : CVE-2019-8607**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8608**	N/A	A-APP-SAFA-060120/248
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8609**	N/A	A-APP-SAFA-060120/249
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS	N/A	A-APP-SAFA-060120/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8610**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8611**	N/A	A-APP-SAFA-060120/251
Out-of-bounds Read	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8615**	N/A	A-APP-SAFA-060120/252
Improper Restriction of Operations	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS	N/A	A-APP-SAFA-060120/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8619**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8622**	N/A	A-APP-SAFA-060120/254
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8623**	N/A	A-APP-SAFA-060120/255
Improper Restriction of Operations	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS	N/A	A-APP-SAFA-060120/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8628**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8644**	N/A	A-APP-SAFA-060120/257
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of synchronous page loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8649**	N/A	A-APP-SAFA-060120/258
Improper	18-12-2019	4.3	An inconsistent user	N/A	A-APP-SAFA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			interface issue was addressed with improved state management. This issue is fixed in Safari 13.0.1. Visiting a malicious website may lead to user interface spoofing. **CVE ID : CVE-2019-8654**		060120/259
Out-of-bounds Read	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8658**	N/A	A-APP-SAFA-060120/260
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8666**	N/A	A-APP-SAFA-060120/261
Improper Restriction of	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling.	N/A	A-APP-SAFA-060120/262

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8669**		
Improper Input Validation	18-12-2019	4.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.6, Safari 12.1.2. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2019-8670**	N/A	A-APP-SAFA-060120/263
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8671**	N/A	A-APP-SAFA-060120/264
Improper Restriction of Operations	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS	N/A	A-APP-SAFA-060120/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8672**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8673**	N/A	A-APP-SAFA-060120/266
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13, Safari 13. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8674**	N/A	A-APP-SAFA-060120/267
Improper Restriction of Operations within the Bounds of a	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3,	N/A	A-APP-SAFA-060120/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8676**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8677**	N/A	A-APP-SAFA-060120/269
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8678**	N/A	A-APP-SAFA-060120/270
Improper Restriction of	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling.	N/A	A-APP-SAFA-060120/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8679**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8680**	N/A	A-APP-SAFA-060120/272
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8681**	N/A	A-APP-SAFA-060120/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8683**	N/A	A-APP-SAFA-060120/274
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8684**	N/A	A-APP-SAFA-060120/275
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to	N/A	A-APP-SAFA-060120/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2019-8685**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8686**	N/A	A-APP-SAFA-060120/277
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8687**	N/A	A-APP-SAFA-060120/278
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for	N/A	A-APP-SAFA-060120/279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8688**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8689**	N/A	A-APP-SAFA-060120/280
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of document loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8690**	N/A	A-APP-SAFA-060120/281
Information Exposure	18-12-2019	5	The issue was addressed with improved handling of service worker lifetime. This issue is fixed in Safari 13.0.1. Service workers may leak	N/A	A-APP-SAFA-060120/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			private browsing history. **CVE ID : CVE-2019-8725**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8808**	N/A	A-APP-SAFA-060120/283
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8811**	N/A	A-APP-SAFA-060120/284
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	A-APP-SAFA-060120/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8812		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8813**	N/A	A-APP-SAFA-060120/286
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8814**	N/A	A-APP-SAFA-060120/287
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8815**	N/A	A-APP-SAFA-060120/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8816**	N/A	A-APP-SAFA-060120/289
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8819**	N/A	A-APP-SAFA-060120/290
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	A-APP-SAFA-060120/291

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8820		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8821**	N/A	A-APP-SAFA-060120/292
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8822**	N/A	A-APP-SAFA-060120/293
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	A-APP-SAFA-060120/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8823		
texture					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4	Some analytics data was sent using HTTP rather than HTTPS. This was addressed by no longer sending this analytics data. This issue is fixed in Texture 5.11.10 for iOS, Texture 4.22.0.4 for Android. An attacker in a privileged network position may be able to intercept analytics data. **CVE ID : CVE-2019-8632**	N/A	A-APP-TEXT-060120/295
shazam					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-12-2019	6.8	An injection issue was addressed with improved validation. This issue is fixed in Shazam Android App Version 9.25.0, Shazam iOS App Version 12.11.0. Processing a maliciously crafted URL may lead to arbitrary javascript code execution. **CVE ID : CVE-2019-8792**	N/A	A-APP-SHAZ-060120/296
swiftnio_ssl					
N/A	18-12-2019	7.5	The issue was addressed by signaling that an executable stack is not required. This issue is fixed in SwiftNIO SSL 2.4.1. A SwiftNIO application using TLS may be able to execute arbitrary code. **CVE ID : CVE-2019-8849**	N/A	A-APP-SWIF-060120/297
Asus					
atk_package					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-12-2019	6.9	AsLdrSrv.exe in ASUS ATK Package before V1.0.0061 (for Windows 10 notebook PCs) could lead to unsigned code execution with no additional execution. The user must put an application at a particular path, with a particular file name. **CVE ID : CVE-2019-19235**	https://www.asus.com/Static_WebPage/ASUS-Product-Security-Advisory/	A-ASU-ATK_-060120/298
Atlassian					
jira					
Missing Authorization	18-12-2019	4	The WorkflowResource class removeStatus method in Jira before version 7.13.12, from version 8.0.0 before version 8.4.3, and from version 8.5.0 before version 8.5.2 allows authenticated remote attackers who do not have project administration access to remove a configured issue status from a project via a missing authorisation check. **CVE ID : CVE-2019-15013**	N/A	A-ATL-JIRA-060120/299
application_links					
Incorrect Default Permissions	17-12-2019	4	The ListEntityLinksServlet resource in Application Links before version 5.0.12, from version 5.1.0 before version 5.2.11, from version 5.3.0 before version 5.3.7, from version 5.4.0 before 5.4.13, and from version 6.0.0 before 6.0.5 disclosed application link information to non-admin users via a missing permissions check.	N/A	A-ATL-APPL-060120/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15011		
backdropcms					
backdrop_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-12-2019	3.5	An issue was discovered in Backdrop CMS 1.13.x before 1.13.5 and 1.14.x before 1.14.2. It doesn't sufficiently filter output when displaying content type names in the content creation interface. An attacker could potentially craft a specialized content type name, then have an editor execute scripting when creating content, aka XSS. This vulnerability is mitigated by the fact that an attacker must have a role with the "Administer content types" permission. **CVE ID : CVE-2019-19900**	N/A	A-BAC-BACK-060120/301
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-12-2019	3.5	An issue was discovered in Backdrop CMS 1.13.x before 1.13.5 and 1.14.x before 1.14.2. It doesn't sufficiently filter output when displaying certain block descriptions created by administrators. An attacker could potentially craft a specialized description, then have an administrator execute scripting when configuring a layout, aka XSS. This issue is mitigated by the fact that the attacker would be required to have the permission to create custom blocks, which is typically an administrative	N/A	A-BAC-BACK-060120/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			task. **CVE ID : CVE-2019-19901**		
Information Exposure	19-12-2019	6.5	An issue was discovered in Backdrop CMS 1.13.x before 1.13.5 and 1.14.x before 1.14.2. It allows the upload of entire-site configuration archives through the user interface or command line. It does not sufficiently check uploaded archives for invalid data, allowing non-configuration scripts to potentially be uploaded to the server. This issue is mitigated by the fact that the attacker would be required to have the "Synchronize, import, and export configuration" permission, a permission that only trusted administrators should be given. Other measures in the product prevent the execution of PHP scripts, so another server-side scripting language must be accessible on the server to execute code. **CVE ID : CVE-2019-19902**	N/A	A-BAC-BACK-060120/303
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-12-2019	3.5	An issue was discovered in Backdrop CMS 1.14.x before 1.14.2. It doesn't sufficiently filter output when displaying file type descriptions created by administrators. An attacker could potentially craft a specialized description, then have an administrator execute	N/A	A-BAC-BACK-060120/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scripting when viewing the list of file types, aka XSS. This vulnerability is mitigated by the fact that an attacker must have a role with the "Administer file types" permission. **CVE ID : CVE-2019-19903**		
centos-webpanel					
centos_web_panel					
Insufficiently Protected Credentials	17-12-2019	4	CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.856 through 0.9.8.864 allows an attacker to get a victim's session file name from the /tmp directory, and the victim's token value from /usr/local/cwpsrv/logs/access_log, then use them to make a request to extract the victim's password (for the OS and phpMyAdmin) via an attacker account. **CVE ID : CVE-2019-14782**	N/A	A-CEN-CENT-060120/305
Insufficiently Protected Credentials	17-12-2019	4	CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.864 allows an attacker to get a victim's session file name from /home/[USERNAME]/tmp/session/sess_xxxxxx, and the victim's token value from /usr/local/cwpsrv/logs/access_log, then use them to gain access to the victim's password (for the OS and phpMyAdmin) via an attacker account. This is different from CVE-2019-	N/A	A-CEN-CENT-060120/306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			14782. **CVE ID : CVE-2019-15235**		
Contao					
contao					
Unrestricted Upload of File with Dangerous Type	17-12-2019	6.5	Contao 4.0 through 4.8.5 allows PHP local file inclusion. A back end user with access to the form generator can upload arbitrary files and execute them on the server. **CVE ID : CVE-2019-19745**	https://contao.org/en/security-advisories/unrestricted-file-uploads.html	A-CON-CONT-060120/307
Improper Encoding or Escaping of Output	17-12-2019	5	Contao 4.8.4 and 4.8.5 has Improper Encoding or Escaping of Output. It is possible to inject insert tags into the login module which will be replaced when the page is rendered. **CVE ID : CVE-2019-19714**	https://contao.org/en/security-advisories/insert-tag-injection-in-the-login-module.html	A-CON-CONT-060120/308
cridio					
listingpro					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-12-2019	4.3	The ListingPro theme before v2.0.14.2 for WordPress has Reflected XSS via the What field on the homepage. **CVE ID : CVE-2019-19540**	N/A	A-CRI-LIST-060120/309
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-12-2019	3.5	The ListingPro theme before v2.0.14.2 for WordPress has Persistent XSS via the Good For field on the new listing submit page. **CVE ID : CVE-2019-19542**	N/A	A-CRI-LIST-060120/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
cwi					
nethack					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-12-2019	7.5	In NatHack between 3.6.0 and 3.6.3, a buffer overflow issue exists when reading very long lines from a NetHack configuration file (usually named .nethackrc). This vulnerability affects systems that have NetHack installed suid/sgid and shared systems that allow users to upload their own configuration files. All users are urged to upgrade to NetHack 3.6.4 as soon as possible. **CVE ID : CVE-2019-16787**	https://github.com/NetHack/NetHack/security/advisories/GHSA-3cm7-rgh5-9pq5	A-CWI-NETH-060120/311
Cybozu					
office					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-12-2019	4	Directory traversal vulnerability in Cybozu Office 10.0.0 to 10.8.3 allows remote authenticated attackers to alter arbitrary files via the 'Customapp' function. **CVE ID : CVE-2019-6022**	N/A	A-CYB-OFFI-060120/312
Cyrus					
imap					
Improper Input Validation	16-12-2019	3.5	An issue was discovered in Cyrus IMAP before 2.5.15, 3.0.x before 3.0.13, and 3.1.x through 3.1.8. If sieve script uploading is allowed (3.x) or certain non-default sieve options are enabled (2.x), a	N/A	A-CYR-IMAP-060120/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user with a mail account on the service can use a sieve script containing a fileinto directive to create any mailbox with administrator privileges, because of folder mishandling in autosieve_createfolder() in imap/lmtp_sieve.c. **CVE ID : CVE-2019-19783**		
Dell					
rsa_identity_governance_and_lifecycle					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	3.5	The RSA Identity Governance and Lifecycle and RSA Via Lifecycle and Governance products prior to 7.1.1 P03 contain a reflected cross-site scripting vulnerability in the My Access Live module [MAL]. An authenticated malicious local user could potentially exploit this vulnerability by sending crafted URL with scripts. When victim users access the module through their browsers, the malicious code gets injected and executed by the web browser in the context of the vulnerable web application. **CVE ID : CVE-2019-18571**	N/A	A-DEL-RSA_-060120/314
Improper Authentication	18-12-2019	7.5	The RSA Identity Governance and Lifecycle and RSA Via Lifecycle and Governance products prior to 7.1.1 P03 contain an Improper Authentication vulnerability. A Java JMX	N/A	A-DEL-RSA_-060120/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			agent running on the remote host is configured with plain text password authentication. An unauthenticated remote attacker can connect to the JMX agent and monitor and manage the Java application. **CVE ID : CVE-2019-18572**		
Djangoproject					
django					
Weak Password Recovery Mechanism for Forgotten Password	18-12-2019	5	Django before 1.11.27, 2.x before 2.2.9, and 3.x before 3.0.1 allows account takeover. A suitably crafted email address (that is equal to an existing user's email address after case transformation of Unicode characters) would allow an attacker to be sent a password reset token for the matched user account. (One mitigation in the new releases is to send password reset tokens only to the registered user email address.) **CVE ID : CVE-2019-19844**	https://www.djangoproject.com/weblog/2019/dec/18/security-releases/	A-DJA-DJAN-060120/316
Drupal					
views_dynamic_field					
Deserialization of Untrusted Data	16-12-2019	7.5	The Views Dynamic Fields module through 7.x-1.0-alpha4 for Drupal makes insecure unserialize calls in handlers/views_handler_filter_dynamic_fields.inc, as demonstrated by PHP object injection, involving a	N/A	A-DRU-VIEW-060120/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			field_names object and an Archive_Tar object, for file deletion. Code execution might also be possible. **CVE ID : CVE-2019-19826**		
Eclipse					
che					
Cross-Site Request Forgery (CSRF)	19-12-2019	6.8	For Eclipse Che versions 6.16 to 7.3.0, with both authentication and TLS disabled, visiting a malicious web site could trigger the start of an arbitrary Che workspace. Che with no authentication and no TLS is not usually deployed on a public network but is often used for local installations (e.g. on personal laptops). In that case, even if the Che API is not exposed externally, some javascript running in the local browser is able to send requests to it. **CVE ID : CVE-2019-17633**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=551596	A-ECL-CHE-060120/318
Elasticsearch					
kibana					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	3.5	Kibana versions before 6.8.6 and 7.5.1 contain a cross site scripting (XSS) flaw in the coordinate and region map visualizations. An attacker with the ability to create coordinate map visualizations could create a malicious visualization. If another Kibana user views that visualization or a dashboard containing the	N/A	A-ELA-KIBA-060120/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			visualization it could execute JavaScript in the victim?s browser. **CVE ID : CVE-2019-7621**		
elog_project					
elog					
Information Exposure	17-12-2019	5	ELOG 3.1.4-57bea22 and below is affected by an information disclosure vulnerability. A remote unauthenticated attacker can access the server's configuration file by sending an HTTP GET request. Amongst the configuration data, the attacker may gain access to valid admin usernames and, in older versions of ELOG, passwords. **CVE ID : CVE-2019-3992**	N/A	A-ELO-ELOG-060120/320
Information Exposure	17-12-2019	5	ELOG 3.1.4-57bea22 and below is affected by an information disclosure vulnerability. A remote unauthenticated attacker can recover a user's password hash by sending a crafted HTTP POST request. **CVE ID : CVE-2019-3993**	N/A	A-ELO-ELOG-060120/321
Use After Free	17-12-2019	5	ELOG 3.1.4-57bea22 and below is affected by a denial of service vulnerability due to a use after free. A remote unauthenticated attacker can crash the ELOG server by sending multiple HTTP POST requests which causes the ELOG function	N/A	A-ELO-ELOG-060120/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			retrieve_url() to use a freed variable. **CVE ID : CVE-2019-3994**		
NULL Pointer Dereference	17-12-2019	5	ELOG 3.1.4-57bea22 and below is affected by a denial of service vulnerability due to a NULL pointer dereference. A remote unauthenticated attacker can crash the ELOG server by sending a crafted HTTP GET request. **CVE ID : CVE-2019-3995**	N/A	A-ELO-ELOG-060120/323
Externally Controlled Reference to a Resource in Another Sphere	17-12-2019	7.5	ELOG 3.1.4-57bea22 and below can be used as an HTTP GET request proxy when unauthenticated remote attackers send crafted HTTP POST requests. **CVE ID : CVE-2019-3996**	N/A	A-ELO-ELOG-060120/324
equinoxce					
control_expert					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-12-2019	7.5	Equinox Control Expert all versions, is vulnerable to an SQL injection attack, which may allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2019-18234**	N/A	A-EQU-CONT-060120/325
excon_project					
excon					
Improper Input Validation	16-12-2019	4.3	In RubyGem excon before 0.71.0, there was a race condition around persistent connections, where a connection which is	https://github.com/excon/excon/security/advisories/GHS	A-EXC-EXCO-060120/326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interrupted (such as by a timeout) would leave data on the socket. Subsequent requests would then read this data, returning content from the previous response. The race condition window appears to be short, and it would be difficult to purposefully exploit this. **CVE ID : CVE-2019-16779**	A-q58g-455p-8vw9	
F5					
big-ip_access_policy_manager					
Information Exposure Through Log Files	23-12-2019	3.5	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, the BIG-IP APM system logs the client-session-id when a per-session policy is attached to the virtual server with debug logging enabled. **CVE ID : CVE-2019-19150**	https://support.f5.com/csp/article/K37890841	A-F5-BIG--060120/327
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	https://support.f5.com/csp/article/K92002212	A-F5-BIG--060120/328
Improper Input Validation	23-12-2019	5	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, under certain conditions when using custom TCP congestion control settings in a TCP profile, TMM stops	https://support.f5.com/csp/article/K06747393	A-F5-BIG--060120/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing traffic when processed by an iRule. **CVE ID : CVE-2019-6677**		
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled. **CVE ID : CVE-2019-6678**	https://support.f5.com/csp/article/K04897373	A-F5-BIG--060120/330
Improper Input Validation	23-12-2019	7.8	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5, while processing traffic through a standard virtual server that targets a FastL4 virtual server (VIP on VIP), hardware appliances may stop responding. **CVE ID : CVE-2019-6680**	https://support.f5.com/csp/article/K53183580	A-F5-BIG--060120/331
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions. **CVE ID : CVE-2019-6683**	https://support.f5.com/csp/article/K76328112	A-F5-BIG--060120/332
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, under certain conditions, a multi-bladed BIG-IP Virtual Clustered Multiprocessing	https://support.f5.com/csp/article/K95117754	A-F5-BIG--060120/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(vCMP) may drop broadcast packets when they are rebroadcast to the vCMP guest secondary blades. An attacker can leverage the fragmented broadcast IP packets to perform any type of fragmentation-based attack. **CVE ID : CVE-2019-6684**		
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/334
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**	https://support.f5.com/csp/article/K25607522	A-F5-BIG--060120/335
big-ip_advanced_firewall_manager					
Improper	23-12-2019	5	On versions 15.0.0-15.0.1,	https://sup	A-F5-BIG--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	port.f5.com /csp/article /K92002212	060120/336
Improper Input Validation	23-12-2019	5	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, under certain conditions when using custom TCP congestion control settings in a TCP profile, TMM stops processing traffic when processed by an iRule. **CVE ID : CVE-2019-6677**	https://support.f5.com /csp/article /K06747393	A-F5-BIG--060120/337
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled. **CVE ID : CVE-2019-6678**	https://support.f5.com /csp/article /K04897373	A-F5-BIG--060120/338
Improper Input Validation	23-12-2019	7.8	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5, while processing traffic through a standard virtual server that targets a FastL4 virtual server (VIP on VIP), hardware appliances may stop responding. **CVE ID : CVE-2019-6680**	https://support.f5.com /csp/article /K53183580	A-F5-BIG--060120/339
Uncontrolled Resource	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2,	https://support.f5.com /csp/article	A-F5-BIG--060120/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions. **CVE ID : CVE-2019-6683**	/K76328112	
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, under certain conditions, a multi-bladed BIG-IP Virtual Clustered Multiprocessing (vCMP) may drop broadcast packets when they are rebroadcast to the vCMP guest secondary blades. An attacker can leverage the fragmented broadcast IP packets to perform any type of fragmentation-based attack. **CVE ID : CVE-2019-6684**	https://support.f5.com/csp/article/K95117754	A-F5-BIG--060120/341
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/342
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2,	https://support.f5.com	A-F5-BIG--060120/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**	/csp/article/K25607522	
big-ip_analytics					
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	https://support.f5.com/csp/article/K92002212	A-F5-BIG--060120/344
Improper Input Validation	23-12-2019	5	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, under certain conditions when using custom TCP congestion control settings in a TCP profile, TMM stops processing traffic when processed by an iRule. **CVE ID : CVE-2019-6677**	https://support.f5.com/csp/article/K06747393	A-F5-BIG--060120/345
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled.	https://support.f5.com/csp/article/K04897373	A-F5-BIG--060120/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6678		
Improper Input Validation	23-12-2019	7.8	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5, while processing traffic through a standard virtual server that targets a FastL4 virtual server (VIP on VIP), hardware appliances may stop responding. **CVE ID : CVE-2019-6680**	https://support.f5.com/csp/article/K53183580	A-F5-BIG--060120/347
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions. **CVE ID : CVE-2019-6683**	https://support.f5.com/csp/article/K76328112	A-F5-BIG--060120/348
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, under certain conditions, a multi-bladed BIG-IP Virtual Clustered Multiprocessing (vCMP) may drop broadcast packets when they are rebroadcast to the vCMP guest secondary blades. An attacker can leverage the fragmented broadcast IP packets to perform any type of fragmentation-based attack.	https://support.f5.com/csp/article/K95117754	A-F5-BIG--060120/349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6684		
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/350
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**	https://support.f5.com/csp/article/K25607522	A-F5-BIG--060120/351
big-ip_application_acceleration_manager					
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	https://support.f5.com/csp/article/K92002212	A-F5-BIG--060120/352
Improper Input	23-12-2019	5	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-	https://support.f5.com	A-F5-BIG--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, under certain conditions when using custom TCP congestion control settings in a TCP profile, TMM stops processing traffic when processed by an iRule. **CVE ID : CVE-2019-6677**	/csp/article/K06747393	060120/353
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled. **CVE ID : CVE-2019-6678**	https://support.f5.com/csp/article/K04897373	A-F5-BIG--060120/354
Improper Input Validation	23-12-2019	7.8	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5, while processing traffic through a standard virtual server that targets a FastL4 virtual server (VIP on VIP), hardware appliances may stop responding. **CVE ID : CVE-2019-6680**	https://support.f5.com/csp/article/K53183580	A-F5-BIG--060120/355
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions. **CVE ID : CVE-2019-6683**	https://support.f5.com/csp/article/K76328112	A-F5-BIG--060120/356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, under certain conditions, a multi-bladed BIG-IP Virtual Clustered Multiprocessing (vCMP) may drop broadcast packets when they are rebroadcast to the vCMP guest secondary blades. An attacker can leverage the fragmented broadcast IP packets to perform any type of fragmentation-based attack. **CVE ID : CVE-2019-6684**	https://support.f5.com/csp/article/K95117754	A-F5-BIG--060120/357
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/358
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the	https://support.f5.com/csp/article/K25607522	A-F5-BIG--060120/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**		
big-ip_application_security_manager					
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	https://support.f5.com/csp/article/K92002212	A-F5-BIG--060120/360
Improper Input Validation	23-12-2019	5	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, under certain conditions when using custom TCP congestion control settings in a TCP profile, TMM stops processing traffic when processed by an iRule. **CVE ID : CVE-2019-6677**	https://support.f5.com/csp/article/K06747393	A-F5-BIG--060120/361
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled. **CVE ID : CVE-2019-6678**	https://support.f5.com/csp/article/K04897373	A-F5-BIG--060120/362
Improper Input Validation	23-12-2019	7.8	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5, while processing traffic through a standard virtual server that targets a	https://support.f5.com/csp/article/K53183580	A-F5-BIG--060120/363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastL4 virtual server (VIP on VIP), hardware appliances may stop responding. **CVE ID : CVE-2019-6680**		
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, the BIG-IP ASM system may consume excessive resources when processing certain types of HTTP responses from the origin web server. This vulnerability is only known to affect resource-constrained systems in which the security policy is configured with response-side features, such as Data Guard or response-side learning. **CVE ID : CVE-2019-6682**	https://support.f5.com/csp/article/K40452417	A-F5-BIG--060120/364
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions. **CVE ID : CVE-2019-6683**	https://support.f5.com/csp/article/K76328112	A-F5-BIG--060120/365
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, under certain conditions, a multi-bladed BIG-IP Virtual	https://support.f5.com/csp/article/K95117754	A-F5-BIG--060120/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Clustered Multiprocessing (vCMP) may drop broadcast packets when they are rebroadcast to the vCMP guest secondary blades. An attacker can leverage the fragmented broadcast IP packets to perform any type of fragmentation-based attack. **CVE ID : CVE-2019-6684**		
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/367
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**	https://support.f5.com/csp/article/K25607522	A-F5-BIG--060120/368
big-ip_domain_name_system					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	https://support.f5.com/csp/article/K92002212	A-F5-BIG--060120/369
Improper Input Validation	23-12-2019	5	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, under certain conditions when using custom TCP congestion control settings in a TCP profile, TMM stops processing traffic when processed by an iRule. **CVE ID : CVE-2019-6677**	https://support.f5.com/csp/article/K06747393	A-F5-BIG--060120/370
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled. **CVE ID : CVE-2019-6678**	https://support.f5.com/csp/article/K04897373	A-F5-BIG--060120/371
Improper Input Validation	23-12-2019	7.8	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5, while processing traffic through a standard virtual server that targets a FastL4 virtual server (VIP on VIP), hardware appliances may stop responding. **CVE ID : CVE-2019-6680**	https://support.f5.com/csp/article/K53183580	A-F5-BIG--060120/372
Uncontrolled Resource	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-	https://support.f5.com	A-F5-BIG--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions. **CVE ID : CVE-2019-6683**	/csp/article/K76328112	060120/373
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, under certain conditions, a multi-bladed BIG-IP Virtual Clustered Multiprocessing (vCMP) may drop broadcast packets when they are rebroadcast to the vCMP guest secondary blades. An attacker can leverage the fragmented broadcast IP packets to perform any type of fragmentation-based attack. **CVE ID : CVE-2019-6684**	https://support.f5.com/csp/article/K95117754	A-F5-BIG--060120/374
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/375
Information	23-12-2019	4	On BIG-IP versions 15.0.0-	https://sup	A-F5-BIG--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**	port.f5.com/csp/article/K25607522	060120/376
big-ip_edge_gateway					
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	https://support.f5.com/csp/article/K92002212	A-F5-BIG--060120/377
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled. **CVE ID : CVE-2019-6678**	https://support.f5.com/csp/article/K04897373	A-F5-BIG--060120/378
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under	https://support.f5.com/csp/article/K76328112	A-F5-BIG--060120/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			undisclosed conditions. **CVE ID : CVE-2019-6683**		
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/380
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**	https://support.f5.com/csp/article/K25607522	A-F5-BIG--060120/381
big-ip_fraud_protection_service					
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	https://support.f5.com/csp/article/K92002212	A-F5-BIG--060120/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-12-2019	5	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, under certain conditions when using custom TCP congestion control settings in a TCP profile, TMM stops processing traffic when processed by an iRule. **CVE ID : CVE-2019-6677**	https://support.f5.com/csp/article/K06747393	A-F5-BIG--060120/383
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled. **CVE ID : CVE-2019-6678**	https://support.f5.com/csp/article/K04897373	A-F5-BIG--060120/384
Improper Input Validation	23-12-2019	7.8	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5, while processing traffic through a standard virtual server that targets a FastL4 virtual server (VIP on VIP), hardware appliances may stop responding. **CVE ID : CVE-2019-6680**	https://support.f5.com/csp/article/K53183580	A-F5-BIG--060120/385
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions.	https://support.f5.com/csp/article/K763281112	A-F5-BIG--060120/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6683		
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, under certain conditions, a multi-bladed BIG-IP Virtual Clustered Multiprocessing (vCMP) may drop broadcast packets when they are rebroadcast to the vCMP guest secondary blades. An attacker can leverage the fragmented broadcast IP packets to perform any type of fragmentation-based attack. **CVE ID : CVE-2019-6684**	https://support.f5.com/csp/article/K95117754	A-F5-BIG--060120/387
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/388
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while	https://support.f5.com/csp/article/K25607522	A-F5-BIG--060120/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**		
big-ip_global_traffic_manager					
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	https://support.f5.com/csp/article/K92002212	A-F5-BIG--060120/390
Improper Input Validation	23-12-2019	5	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, under certain conditions when using custom TCP congestion control settings in a TCP profile, TMM stops processing traffic when processed by an iRule. **CVE ID : CVE-2019-6677**	https://support.f5.com/csp/article/K06747393	A-F5-BIG--060120/391
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled. **CVE ID : CVE-2019-6678**	https://support.f5.com/csp/article/K04897373	A-F5-BIG--060120/392
Improper Input Validation	23-12-2019	7.8	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5, while processing traffic through a standard	https://support.f5.com/csp/article/K53183580	A-F5-BIG--060120/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			virtual server that targets a FastL4 virtual server (VIP on VIP), hardware appliances may stop responding. **CVE ID : CVE-2019-6680**		
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions. **CVE ID : CVE-2019-6683**	https://support.f5.com/csp/article/K76328112	A-F5-BIG--060120/394
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, under certain conditions, a multi-bladed BIG-IP Virtual Clustered Multiprocessing (vCMP) may drop broadcast packets when they are rebroadcast to the vCMP guest secondary blades. An attacker can leverage the fragmented broadcast IP packets to perform any type of fragmentation-based attack. **CVE ID : CVE-2019-6684**	https://support.f5.com/csp/article/K95117754	A-F5-BIG--060120/395
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**		
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**	https://support.f5.com/csp/article/K25607522	A-F5-BIG--060120/397
big-ip_link_controller					
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	https://support.f5.com/csp/article/K92002212	A-F5-BIG--060120/398
Improper Input Validation	23-12-2019	5	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, under certain conditions when using custom TCP congestion control settings in a TCP profile, TMM stops processing traffic when	https://support.f5.com/csp/article/K06747393	A-F5-BIG--060120/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processed by an iRule. **CVE ID : CVE-2019-6677**		
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled. **CVE ID : CVE-2019-6678**	https://support.f5.com/csp/article/K04897373	A-F5-BIG--060120/400
Improper Input Validation	23-12-2019	7.8	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5, while processing traffic through a standard virtual server that targets a FastL4 virtual server (VIP on VIP), hardware appliances may stop responding. **CVE ID : CVE-2019-6680**	https://support.f5.com/csp/article/K53183580	A-F5-BIG--060120/401
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions. **CVE ID : CVE-2019-6683**	https://support.f5.com/csp/article/K76328112	A-F5-BIG--060120/402
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, under certain conditions, a multi-bladed BIG-IP Virtual Clustered Multiprocessing (vCMP) may drop broadcast	https://support.f5.com/csp/article/K95117754	A-F5-BIG--060120/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets when they are rebroadcast to the vCMP guest secondary blades. An attacker can leverage the fragmented broadcast IP packets to perform any type of fragmentation-based attack. **CVE ID : CVE-2019-6684**		
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/404
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**	https://support.f5.com/csp/article/K25607522	A-F5-BIG--060120/405
big-ip_local_traffic_manager					
Improper Input	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-	https://support.f5.com	A-F5-BIG--060120/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	/csp/article/K92002212	
Improper Input Validation	23-12-2019	5	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, under certain conditions when using custom TCP congestion control settings in a TCP profile, TMM stops processing traffic when processed by an iRule. **CVE ID : CVE-2019-6677**	https://support.f5.com/csp/article/K06747393	A-F5-BIG--060120/407
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled. **CVE ID : CVE-2019-6678**	https://support.f5.com/csp/article/K04897373	A-F5-BIG--060120/408
Improper Input Validation	23-12-2019	7.8	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5, while processing traffic through a standard virtual server that targets a FastL4 virtual server (VIP on VIP), hardware appliances may stop responding. **CVE ID : CVE-2019-6680**	https://support.f5.com/csp/article/K53183580	A-F5-BIG--060120/409
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-	https://support.f5.com/csp/article/K7632811	A-F5-BIG--060120/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions. **CVE ID : CVE-2019-6683**	2	
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, under certain conditions, a multi-bladed BIG-IP Virtual Clustered Multiprocessing (vCMP) may drop broadcast packets when they are rebroadcast to the vCMP guest secondary blades. An attacker can leverage the fragmented broadcast IP packets to perform any type of fragmentation-based attack. **CVE ID : CVE-2019-6684**	https://support.f5.com/csp/article/K95117754	A-F5-BIG--060120/411
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/412
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-	https://support.f5.com/csp/article	A-F5-BIG--060120/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**	/K25607522	
big-ip_policy_enforcement_manager					
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	https://support.f5.com/csp/article/K92002212	A-F5-BIG--060120/414
Improper Input Validation	23-12-2019	5	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, under certain conditions when using custom TCP congestion control settings in a TCP profile, TMM stops processing traffic when processed by an iRule. **CVE ID : CVE-2019-6677**	https://support.f5.com/csp/article/K06747393	A-F5-BIG--060120/415
Improper Input Validation	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled.	https://support.f5.com/csp/article/K04897373	A-F5-BIG--060120/416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6678		
Improper Input Validation	23-12-2019	7.8	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5, while processing traffic through a standard virtual server that targets a FastL4 virtual server (VIP on VIP), hardware appliances may stop responding. **CVE ID : CVE-2019-6680**	https://support.f5.com/csp/article/K53183580	A-F5-BIG--060120/417
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions. **CVE ID : CVE-2019-6683**	https://support.f5.com/csp/article/K76328112	A-F5-BIG--060120/418
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1.1, 14.0.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, under certain conditions, a multi-bladed BIG-IP Virtual Clustered Multiprocessing (vCMP) may drop broadcast packets when they are rebroadcast to the vCMP guest secondary blades. An attacker can leverage the fragmented broadcast IP packets to perform any type of fragmentation-based attack.	https://support.f5.com/csp/article/K95117754	A-F5-BIG--060120/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6684		
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/420
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**	https://support.f5.com/csp/article/K25607522	A-F5-BIG--060120/421
big-ip_webaccelerator					
Improper Input Validation	23-12-2019	5	On versions 15.0.0-15.0.1, 14.0.0-14.1.2.2, and 13.1.0-13.1.3.1, TMM may restart on BIG-IP Virtual Edition (VE) when using virtio direct descriptors and packets 2 KB or larger. **CVE ID : CVE-2019-6676**	https://support.f5.com/csp/article/K92002212	A-F5-BIG--060120/422
Improper Input	23-12-2019	4.3	On BIG-IP versions 15.0.0-15.0.1, 14.1.0-14.1.2.2,	https://support.f5.com	A-F5-BIG--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			14.0.0-14.0.1, and 13.1.0-13.1.3.1, the TMM process may restart when the packet filter feature is enabled. **CVE ID : CVE-2019-6678**	/csp/article/K04897373	060120/423
Uncontrolled Resource Consumption	23-12-2019	4.3	On versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, BIG-IP virtual servers with Loose Initiation enabled on a FastL4 profile may be subject to excessive flow usage under undisclosed conditions. **CVE ID : CVE-2019-6683**	https://support.f5.com/csp/article/K76328112	A-F5-BIG--060120/424
Improper Privilege Management	23-12-2019	4.6	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, users with access to edit iRules are able to create iRules which can lead to an elevation of privilege, configuration modification, and arbitrary system command execution. **CVE ID : CVE-2019-6685**	https://support.f5.com/csp/article/K30215839	A-F5-BIG--060120/425
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the	https://support.f5.com/csp/article/K25607522	A-F5-BIG--060120/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**		
big-iq_centralized_management					
Information Exposure	23-12-2019	4	On BIG-IP versions 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5 and BIG-IQ versions 6.0.0-6.1.0 and 5.2.0-5.4.0, a user is able to obtain the secret that was being used to encrypt a BIG-IP UCS backup file while sending SNMP query to the BIG-IP or BIG-IQ system, however the user can not access to the UCS files. **CVE ID : CVE-2019-6688**	https://support.f5.com/csp/article/K25607522	A-F5-BIG--060120/427
ffjpeg_project					
ffjpeg					
NULL Pointer Dereference	18-12-2019	4.3	bitstr_tell at bitstr.c in ffjpeg through 2019-08-21 has a NULL pointer dereference related to jfif_encode. **CVE ID : CVE-2019-19887**	N/A	A-FFJ-FFJP-060120/428
Divide By Zero	18-12-2019	4.3	jfif_decode in jfif.c in ffjpeg through 2019-08-21 has a divide-by-zero error. **CVE ID : CVE-2019-19888**	N/A	A-FFJ-FFJP-060120/429
getk2					
k2					
Unrestricted Upload of File with Dangerous	17-12-2019	7.5	class.upload.php in verot.net class.upload through 1.0.3 and 2.x through 2.0.4, as used in the K2 extension for	N/A	A-GET-K2-060120/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			Joomla! and other products, omits .pht from the set of dangerous file extensions, a similar issue to CVE-2019-19576. **CVE ID : CVE-2019-19634**		
GIT					
git					
Improper Input Validation	18-12-2019	6.8	An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. Recursive clones are currently affected by a vulnerability that is caused by too-lax validation of submodule names, allowing very targeted attacks via remote code execution in recursive clones. **CVE ID : CVE-2019-1387**	https://lore.kernel.org/git/xmqqr21cqcn9.fsf@gitster-ct.c.googlers.com/T/#u	A-GIT-GIT-060120/431
Gitlab					
gitlab					
N/A	18-12-2019	6.5	An improper access control vulnerability exists in Gitlab <v12.3.2, <v12.2.6, <v12.1.12 which would allow a blocked user would be able to use GIT clone and pull if he had obtained a CI/CD token before. **CVE ID : CVE-2019-15589**	N/A	A-GIT-GITL-060120/432
Information Exposure	18-12-2019	4	An improper access control vulnerability exists in GitLab <12.3.3 that allows an attacker to obtain container and dependency scanning	N/A	A-GIT-GITL-060120/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reports through the merge request widget even though public pipelines were disabled. **CVE ID : CVE-2019-15591**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-12-2019	5	A command injection exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed an attacker to inject commands via the API through the blobs scope. **CVE ID : CVE-2019-15575**	N/A	A-GIT-GITL-060120/434
Information Exposure	18-12-2019	5	An information disclosure vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed an attacker to view private system notes from a GraphQL endpoint. **CVE ID : CVE-2019-15576**	N/A	A-GIT-GITL-060120/435
Information Exposure	18-12-2019	4	An information disclosure vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed project milestones to be disclosed via groups browsing. **CVE ID : CVE-2019-15577**	N/A	A-GIT-GITL-060120/436
Information Exposure	18-12-2019	4	An information exposure vulnerability exists in gitlab.com <v12.3.2, <v12.2.6, and <v12.1.10 when using the blocking merge request feature, it was possible for an unauthenticated user to see the head pipeline data of a	N/A	A-GIT-GITL-060120/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			public project even though pipeline visibility was restricted. **CVE ID : CVE-2019-15580**		
Authorization Bypass Through User-Controlled Key	18-12-2019	5.5	An IDOR vulnerability exists in GitLab <v12.1.2, <v12.0.4, and <v11.11.6 that allowed uploading files from project archive to replace other users files potentially allowing an attacker to replace project binaries or other uploaded assets. **CVE ID : CVE-2019-5469**	N/A	A-GIT-GITL-060120/438
Improper Authentication	18-12-2019	6.5	A authentication bypass vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.10 in the Salesforce login integration that could be used by an attacker to create an account that bypassed domain restrictions and email verification requirements. **CVE ID : CVE-2019-5486**	N/A	A-GIT-GITL-060120/439
Information Exposure	18-12-2019	5	An improper access control vulnerability exists in Gitlab EE <v12.3.3, <v12.2.7, & <v12.1.13 that allowed the group search feature with Elasticsearch to return private code, merge requests and commits. **CVE ID : CVE-2019-5487**	N/A	A-GIT-GITL-060120/440
GNU					
libredwg					
Uncontrolled Resource	27-12-2019	4.3	An issue was discovered in GNU LibreDWG before 0.93.	N/A	A-GNU-LIBR-060120/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			Crafted input will lead to an attempted excessive memory allocation in dwg_decode_SPLINE_private in dwg.spec. **CVE ID : CVE-2019-20009**		
Use After Free	27-12-2019	6.8	An issue was discovered in GNU LibreDWG 0.92. There is a use-after-free in resolve_objectref_vector in decode.c. **CVE ID : CVE-2019-20010**	N/A	A-GNU-LIBR-060120/442
Out-of-bounds Read	27-12-2019	6.8	An issue was discovered in GNU LibreDWG 0.92. There is a heap-based buffer over-read in decode_R13_R2000 in decode.c. **CVE ID : CVE-2019-20011**	N/A	A-GNU-LIBR-060120/443
Uncontrolled Resource Consumption	27-12-2019	4.3	An issue was discovered in GNU LibreDWG 0.92. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_HATCH_private in dwg.spec. **CVE ID : CVE-2019-20012**	N/A	A-GNU-LIBR-060120/444
Uncontrolled Resource Consumption	27-12-2019	4.3	An issue was discovered in GNU LibreDWG before 0.93. Crafted input will lead to an attempted excessive memory allocation in decode_3dsolid in dwg.spec. **CVE ID : CVE-2019-20013**	N/A	A-GNU-LIBR-060120/445
Double Free	27-12-2019	6.8	An issue was discovered in GNU LibreDWG before 0.93. There is a double-free in dwg_free in free.c.	N/A	A-GNU-LIBR-060120/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-20014		
Uncontrolled Resource Consumption	27-12-2019	4.3	An issue was discovered in GNU LibreDWG 0.92. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_LWPOLYLINE_ private in dwg.spec. **CVE ID : CVE-2019-20015**	N/A	A-GNU-LIBR-060120/447
gonitro					
nitro_free_pdf_reader					
Out-of-bounds Read	16-12-2019	4.3	The JBIG2Decode library in npdf.dll in Nitro Free PDF Reader 12.0.0.112 has a CAPPDAnnotHandlerUtils::PDAnnotHandlerDestroyData 2+0xa08a Out-of-Bounds Read via crafted Unicode content. **CVE ID : CVE-2019-19818**	N/A	A-GON-NITR-060120/448
Google					
tensorflow					
Out-of-bounds Write	16-12-2019	7.5	In TensorFlow before 1.15, a heap buffer overflow in UnsortedSegmentSum can be produced when the Index template argument is int32. In this case data_size and num_segments fields are truncated from int64 to int32 and can produce negative numbers, resulting in accessing out of bounds heap memory. This is unlikely to be exploitable and was detected and fixed internally in TensorFlow 1.15 and 2.0.	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-844w-j86r-4x2j	A-GOO-TENS-060120/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16778		
handlebars.js_project					
handlebars.js					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-12-2019	7.5	Versions of handlebars prior to 4.3.0 are vulnerable to Prototype Pollution leading to Remote Code Execution. Templates may alter an Object's __proto__ and __defineGetter__ properties, which may allow an attacker to execute arbitrary code through crafted payloads. **CVE ID : CVE-2019-19919**	N/A	A-HAN-HAND-060120/450
hcltech					
appscan_source					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	3.5	HCL AppScan Source 9.0.3.13 and earlier is susceptible to cross-site scripting (XSS) attacks by allowing users to embed arbitrary JavaScript code in the Web UI. **CVE ID : CVE-2019-4388**	https://hclpnpsupport.hcltech.com/csm?id=kb_article&sysparm_article=KB0074364	A-HCL-APPS-060120/451
HP					
oneview_for_vmware_vcenter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A security vulnerability in HPE OneView for VMware vCenter 9.5 could be exploited remotely to allow Cross-Site Scripting. **CVE ID : CVE-2019-11992**	N/A	A-HP-ONEV-060120/452
http_server_project					
http_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-12-2019	5	A Path traversal exists in http_server which allows an attacker to read arbitrary system files. **CVE ID : CVE-2019-15600**	N/A	A-HTT-HTTP-060120/453
IBM					
mq_appliance					
Improper Input Validation	16-12-2019	4	IBM MQ and IBM MQ Appliance 9.1 CD, 9.1 LTS, 9.0 LTS, and 8.0 is vulnerable to a denial of service attack caused by channels processing poorly formatted messages. IBM X-Force ID: 166357. **CVE ID : CVE-2019-4560**	https://www.ibm.com/support/pages/node/1106037	A-IBM-MQ_A-060120/454
planning_analytics					
Incorrect Authorization	18-12-2019	10	IBM Planning Analytics 2.0.0 through 2.0.8 is vulnerable to a configuration overwrite that allows an unauthenticated user to login as "admin", and then execute code as root or SYSTEM via TM1 scripting. IBM X-Force ID: 172094. **CVE ID : CVE-2019-4716**	https://www.ibm.com/support/pages/node/1127781	A-IBM-PLAN-060120/455
cognos_analytics					
Cross-Site Request Forgery (CSRF)	20-12-2019	4.3	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that	https://www.ibm.com/support/pages/node/1138588	A-IBM-COGN-060120/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the website trusts. IBM X-Force ID: 159356. **CVE ID : CVE-2019-4231**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-12-2019	3.5	IBM Cognos Analytics 11.0 and 11.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 166204. **CVE ID : CVE-2019-4555**	https://www.ibm.com/support/pages/node/1138588	A-IBM-COGN-060120/457
api_connect					
Insufficiently Protected Credentials	16-12-2019	2.1	IBM API Connect 2018.1 through 2018.4.1.7 Developer Portal's user registration page does not disable password autocomplete. An attacker with access to the browser instance and local system credentials can steal the credentials used for registration. IBM X-Force ID: 163453. **CVE ID : CVE-2019-4444**	https://www.ibm.com/support/pages/node/1126833	A-IBM-API_-060120/458
Information Exposure	18-12-2019	5	IBM API Connect 2018.4.1.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 168510. **CVE ID : CVE-2019-4609**	https://www.ibm.com/support/pages/node/1137460	A-IBM-API_-060120/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
financial_transaction_manager_for_multiplatform					
Cross-Site Request Forgery (CSRF)	20-12-2019	4.3	IBM Financial Transaction Manager 3.0 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: 172706. **CVE ID : CVE-2019-4736**	https://www.ibm.com/support/pages/node/1135173	A-IBM-FINA-060120/460
Improper Restriction of Rendered UI Layers or Frames	20-12-2019	4.3	IBM Financial Transaction Manager 3.0 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 further attacks against the victim. IBM X-Force ID: 172877. **CVE ID : CVE-2019-4742**	https://www.ibm.com/support/pages/node/1135173	A-IBM-FINA-060120/461
Cleartext Transmission of Sensitive Information	20-12-2019	4.3	IBM Financial Transaction Manager 3.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID:	https://www.ibm.com/support/pages/node/1135173	A-IBM-FINA-060120/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			172880. **CVE ID : CVE-2019-4743**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-12-2019	4.3	IBM Financial Transaction Manager 3.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 172882. **CVE ID : CVE-2019-4744**	https://www.ibm.com/support/pages/node/1135173	A-IBM-FINA-060120/463
icegram					
email_subscribers_\&_newsletters					
Improper Privilege Management	26-12-2019	4	The WordPress plugin, Email Subscribers & Newsletters, before 4.2.3 had a privilege bypass flaw that allowed authenticated users (Subscriber or greater access) to send test emails from the administrative dashboard on behalf of an administrator. This occurs because the plugin registers a wp_ajax function to send_test_email. **CVE ID : CVE-2019-19980**	N/A	A-ICE-EMAI-060120/464
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-12-2019	4.3	The WordPress plugin, Email Subscribers & Newsletters, before 4.2.3 had a flaw that allowed for CSRF to be exploited on all plugin settings. **CVE ID : CVE-2019-19981**	N/A	A-ICE-EMAI-060120/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Improper Authenticati on	26-12-2019	5	The WordPress plugin, Email Subscribers & Newsletters, before 4.2.3 had a flaw that allowed for unauthenticated option creation. In order to exploit this vulnerability, an attacker would need to send a /wp-admin/admin-post.php?es_skip=1&option_name= request. **CVE ID : CVE-2019-19982**	N/A	A-ICE-EMAI-060120/466
Incorrect Permission Assignment for Critical Resource	26-12-2019	6.5	The WordPress plugin, Email Subscribers & Newsletters, before 4.2.3 had a flaw that allowed users with edit_post capabilities to manage plugin settings and email campaigns. **CVE ID : CVE-2019-19984**	N/A	A-ICE-EMAI-060120/467
Information Exposure	26-12-2019	5	The WordPress plugin, Email Subscribers & Newsletters, before 4.2.3 had a flaw that allowed unauthenticated file download with user information disclosure. **CVE ID : CVE-2019-19985**	N/A	A-ICE-EMAI-060120/468
Intel					
quartus_prime					
Incorrect Default Permissions	16-12-2019	4.6	Improper permissions in the installer for the License Server software for Intel? Quartus? Prime Pro Edition before version 19.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	N/A	A-INT-QUAR-060120/469

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-14603		
NULL Pointer Dereference	16-12-2019	2.1	Null pointer dereference in the FPGA kernel driver for Intel(R) Quartus(R) Prime Pro Edition before version 19.3 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2019-14604**	N/A	A-INT-QUAR-060120/470
ethernet_i218_adapter_driver					
Information Exposure	16-12-2019	2.1	Insufficient memory protection for Intel(R) Ethernet I218 Adapter driver for Windows* 10 before version 24.1 may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-11096**	N/A	A-INT-ETHE-060120/471
field_programmable_gate_array_software_development_kit_for_opencl					
Improper Check for Unusual or Exceptional Conditions	16-12-2019	2.1	Improper conditions check in the Linux kernel driver for the Intel(R) FPGA SDK for OpenCL(TM) Pro Edition before version 19.4 may allow an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2019-11165**	https://support.f5.com/csp/article/K07357521?utm_source=f5support&utm_medium=RSS	A-INT-FIEL-060120/472
dynamic_platform_and_thermal_framework					
Incorrect Default Permissions	16-12-2019	4.6	Improper permissions in the Intel(R) Dynamic Platform and Thermal Framework v8.3.10208.5643 and before may allow an authenticated user to potentially execute	N/A	A-INT-DYNA-060120/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code at an elevated level of privilege. **CVE ID : CVE-2019-0134**		
administrative_tools_for_intel_network_adapters					
Improper Privilege Management	16-12-2019	4.6	Insufficient memory protection in the Linux Administrative Tools for Intel(R) Network Adapters before version 24.3 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-0159**	N/A	A-INT-ADMI-060120/474
rapid_storage_technology					
Incorrect Default Permissions	16-12-2019	4.6	Improper permissions in the executable for Intel(R) RST before version 17.7.0.1006 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-14568**	N/A	A-INT-RAPI-060120/475
control_center-i					
Improper Privilege Management	16-12-2019	4.6	Unquoted service path in Control Center-I version 2.1.0.0 and earlier may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-14599**	N/A	A-INT-CONT-060120/476
setup_and_configuration_software_platform_discovery_utility					
Incorrect Default Permissions	16-12-2019	4.6	Improper permissions in the installer for the Intel(R) SCS Platform Discovery Utility, all versions, may allow an authenticated user to	N/A	A-INT-SETU-060120/477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially enable escalation of privilege via local attack. **CVE ID : CVE-2019-14605**		
ivanti					
workspace_control					
Incorrect Default Permissions	17-12-2019	4.4	In Ivanti Workspace Control before 10.3.180.0. a locally authenticated user with low privileges can bypass Managed Application Security by leveraging an unspecified attack vector in Workspace Preferences, when it is enabled. As a result, the attacker can start applications that should be blocked. **CVE ID : CVE-2019-19675**	https://forums.ivanti.com/s/article/Locally-authenticated-user-can-bypass-File-and-Folder-Security-by-leveraging-an-unspecified-attack-vector	A-IVA-WORK-060120/478
Jenkins					
websphere_deployer					
Improper Certificate Validation	17-12-2019	5.5	Jenkins WebSphere Deployer Plugin 1.6.1 and earlier allows users with Overall/Read access to disable SSL/TLS certificate and hostname validation for the entire Jenkins master JVM. **CVE ID : CVE-2019-16561**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1581	A-JEN-WEBS-060120/479
build_graph_view					
Improper Neutralization of Input During Web Page Generation	17-12-2019	3.5	Jenkins buildgraph-view Plugin 1.8 and earlier does not escape the description of builds shown in its view, resulting in a stored XSS vulnerability exploitable by	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1591	A-JEN-BUIL-060120/480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			users able to change build descriptions. **CVE ID : CVE-2019-16562**		
mission_control					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-12-2019	3.5	Jenkins Mission Control Plugin 0.9.16 and earlier does not escape job display names and build names shown on its view, resulting in a stored XSS vulnerability exploitable by attackers able to change these properties. **CVE ID : CVE-2019-16563**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1592	A-JEN-MISS-060120/481
pipeline_aggregator_view					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-12-2019	3.5	Jenkins Pipeline Aggregator View Plugin 1.8 and earlier does not escape information shown on its view, resulting in a stored XSS vulnerability exploitable by attackers able to affects view content such as job display name or pipeline stage names. **CVE ID : CVE-2019-16564**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1593	A-JEN-PIPE-060120/482
team_concert					
Insufficiently Protected Credentials	17-12-2019	4	A missing permission check in Jenkins Team Concert Plugin 1.3.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-16566**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1605%20(1)	A-JEN-TEAM-060120/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	17-12-2019	4	A missing permission check in Jenkins Team Concert Plugin 1.3.0 and earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins. **CVE ID : CVE-2019-16567**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1605%20(2)	A-JEN-TEAM-060120/484
Cross-Site Request Forgery (CSRF)	17-12-2019	6.8	A cross-site request forgery vulnerability in Jenkins Team Concert Plugin 1.3.0 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-16565**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1605%20(1)	A-JEN-TEAM-060120/485
sctmexecutor					
Cleartext Transmission of Sensitive Information	17-12-2019	5	Jenkins SCTMExecutor Plugin 2.2 and earlier transmits previously configured service credentials in plain text as part of the global configuration, as well as individual jobs' configurations. **CVE ID : CVE-2019-16568**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1521	A-JEN-SCTM-060120/486
mantis					
Cross-Site Request Forgery (CSRF)	17-12-2019	4.3	A cross-site request forgery vulnerability in Jenkins Mantis Plugin 0.26 and earlier allows attackers to connect to an attacker-specified web server using	https://jenkins.io/security/advisory/2019-12-17/#SECUR	A-JEN-MANT-060120/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker-specified credentials. **CVE ID : CVE-2019-16569**	ITY-1603	
rapiddeploy					
Cross-Site Request Forgery (CSRF)	17-12-2019	6.8	A cross-site request forgery vulnerability in Jenkins RapidDeploy Plugin 4.1 and earlier allows attackers to connect to an attacker-specified web server. **CVE ID : CVE-2019-16570**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1604	A-JEN-RAPI-060120/488
Incorrect Permission Assignment for Critical Resource	17-12-2019	4	A missing permission check in Jenkins RapidDeploy Plugin 4.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified web server. **CVE ID : CVE-2019-16571**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1604	A-JEN-RAPI-060120/489
weibo					
Insufficiently Protected Credentials	17-12-2019	2.1	Jenkins Weibo Plugin 1.0.1 and earlier stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-16572**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1597	A-JEN-WEIB-060120/490
alauda_devops_pipeline					
Cross-Site Request Forgery (CSRF)	17-12-2019	6.8	A cross-site request forgery vulnerability in Jenkins Alauda DevOps Pipeline Plugin 2.3.2 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1600	A-JEN-ALAU-060120/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-16573**		
Insufficiently Protected Credentials	17-12-2019	4	A missing permission check in Jenkins Alauda DevOps Pipeline Plugin 2.3.2 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2019-16574**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1600	A-JEN-ALAU-060120/492
alauda_kubernetes_support					
Cross-Site Request Forgery (CSRF)	17-12-2019	6.8	A cross-site request forgery vulnerability in Jenkins Alauda Kubernetes Suport Plugin 2.3.0 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing the Kubernetes service account token or credentials stored in Jenkins. **CVE ID : CVE-2019-16575**	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1602	A-JEN-ALAU-060120/493
Insufficiently Protected Credentials	17-12-2019	4	A missing permission check in Jenkins Alauda Kubernetes Suport Plugin 2.3.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified	https://jenkins.io/security/advisory/2019-12-17/#SECURITY-1602	A-JEN-ALAU-060120/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials IDs obtained through another method, capturing the Kubernetes service account token or credentials stored in Jenkins. **CVE ID : CVE-2019-16576**		
Joomla					
joomla\!					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-12-2019	5	In Joomla! before 3.9.14, a missing access check in framework files could lead to a path disclosure. **CVE ID : CVE-2019-19845**	N/A	A-JOO-JOOM-060120/495
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-12-2019	7.5	In Joomla! before 3.9.14, the lack of validation of configuration parameters used in SQL queries caused various SQL injection vectors. **CVE ID : CVE-2019-19846**	N/A	A-JOO-JOOM-060120/496
Lansweeper					
lansweeper					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-12-2019	4.3	The web console in Lansweeper 7.2.105.2 has XSS via the URL path. Product vulnerability has been fixed and disclosed within changelog as of 02 Dec 2019. **CVE ID : CVE-2019-18955**	https://www.lansweeper.com/changelog/	A-LAN-LANS-060120/497
libspiro_project					
libspiro					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-12-2019	7.5	Libspiro through 20190731 has a stack-based buffer overflow in the spiro_to_bpath0() function in spiro.c. **CVE ID : CVE-2019-19847**	N/A	A-LIB-LIBS-060120/498
lout_project					
lout					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-12-2019	6.8	Lout 3.40 has a buffer overflow in the StringQuotedWord() function in z39.c. **CVE ID : CVE-2019-19917**	N/A	A-LOU-LOUT-060120/499
Out-of-bounds Write	20-12-2019	6.8	Lout 3.40 has a heap-based buffer overflow in the srcnext() function in z02.c. **CVE ID : CVE-2019-19918**	N/A	A-LOU-LOUT-060120/500
Maxum					
rumpus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-12-2019	4.3	A Reflected Cross Site Scripting was discovered in the Login page of Rumpus FTP Web File Manager 8.2.9.1. An attacker can exploit it by sending a crafted link to end users and can execute arbitrary Javascripts **CVE ID : CVE-2019-19368**	N/A	A-MAX-RUMP-060120/501
Microfocus					
arcsight_logger					
Cross-Site Request Forgery (CSRF)	17-12-2019	6.8	Cross-Site Request Forgery vulnerability in all Micro Focus ArcSight Logger affecting all product versions	N/A	A-MIC-ARCS-060120/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			below version 7.0. The vulnerability could be exploited to perform CSRF attack. **CVE ID : CVE-2019-11657**		
mz-automation					
libiec61850					
Integer Overflow or Wraparound	23-12-2019	4.3	In libIEC61850 1.4.0, MmsValue_newOctetString in mms/iso_mms/common/mms_value.c has an integer signedness error that can lead to an attempted excessive memory allocation. **CVE ID : CVE-2019-19930**	N/A	A-MZ--LIBI-060120/503
Out-of-bounds Write	23-12-2019	6.8	In libIEC61850 1.4.0, MmsValue_decodeMmsData in mms/iso_mms/server/mms_access_result.c has a heap-based buffer overflow. **CVE ID : CVE-2019-19931**	N/A	A-MZ--LIBI-060120/504
Out-of-bounds Read	23-12-2019	4.3	In libIEC61850 1.4.0, BerDecoder_decodeUint32 in mms/asn1/ber_decode.c has an out-of-bounds read, related to intLen and bufPos. **CVE ID : CVE-2019-19944**	N/A	A-MZ--LIBI-060120/505
nethack					
nethack					
Buffer Copy without Checking Size of Input ('Classic	19-12-2019	7.5	NetHack 3.6.x before 3.6.4 is prone to a buffer overflow vulnerability when reading very long lines from configuration files. This	https://github.com/NetHack/NetHack/security/advisorie	A-NET-NETH-060120/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			affects systems that have NetHack installed suid/sgid, and shared systems that allow users to upload their own configuration files. **CVE ID : CVE-2019-19905**	s/GHSA-3cm7-rgh5-9pq5	
nic					
knot_resolver					
Improper Resource Shutdown or Release	16-12-2019	5	knot-resolver before version 4.3.0 is vulnerable to denial of service through high CPU utilization. DNS replies with very many resource records might be processed very inefficiently, in extreme cases taking even several CPU seconds for each such uncached message. For example, a few thousand A records can be squashed into one DNS message (limit is 64kB). **CVE ID : CVE-2019-19331**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-19331	A-NIC-KNOT-060120/507
node-df_project					
node-df					
Improper Control of Generation of Code ('Code Injection')	18-12-2019	7.5	A code injection exists in node-df v0.1.4 that can allow an attacker to remote code execution by unsanitized input. **CVE ID : CVE-2019-15597**	N/A	A-NOD-NODE-060120/508
Odoo					
odoo					
Improper Privilege Management	19-12-2019	5.5	Improper access control in the computed fields system of the framework of Odoo Community 13.0 and Odoo	N/A	A-ODO-ODOO-060120/509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise 13.0 allows remote authenticated attackers to access sensitive information via crafted RPC requests, which could lead to privilege escalation. **CVE ID : CVE-2019-11780**		
rack_project					
rack					
Information Exposure	18-12-2019	4.3	There's a possible information leak / session hijack vulnerability in Rack (RubyGem rack). This vulnerability is patched in versions 1.6.12 and 2.0.8. Attackers may be able to find and hijack sessions by using timing attacks targeting the session id. Session ids are usually stored and indexed in a database that uses some kind of scheme for speeding up lookups of that session id. By carefully measuring the amount of time it takes to look up a session, an attacker may be able to find a valid session id and hijack the session. The session id itself may be generated randomly, but the way the session is indexed by the backing store does not use a secure comparison. **CVE ID : CVE-2019-16782**	https://github.com/rack/rack/commit/7fecaee81f59926b6e1913511c90650e76673b38, https://github.com/rack/rack/security/advisories/GHSA-hrqr-hxpp-chr3	A-RAC-RACK-060120/510
roxyfileman					
roxy_fileman					
Improper Limitation of	16-12-2019	5	Roxy Fileman 1.4.5 for .NET is vulnerable to path	N/A	A-ROX-ROXY-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			traversal. A remote attacker can write uploaded files to arbitrary locations via the RENAMEFILE action. This can be leveraged for code execution by uploading a specially crafted Windows shortcut file and writing the file to the Startup folder (because an incomplete blacklist of file extensions allows Windows shortcut files to be uploaded). **CVE ID : CVE-2019-19731**		060120/511
SAP					
enterprise_extension_financial_services					
Incorrect Authorization	17-12-2019	6.5	Transaction Management in SAP Treasury and Risk Management (corrected in S4CORE versions 1.01, 1.02, 1.03, 1.04 and EA-FINSERV versions 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2019-0383**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528880390	A-SAP-ENTE-060120/512
Incorrect Authorization	17-12-2019	6.5	Transaction Management in SAP Treasury and Risk Management (corrected in S4CORE versions 1.01, 1.02, 1.03, 1.04 and EA-FINSERV versions 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0) does not perform necessary authorization checks for functionalities that require user identity.	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528880390	A-SAP-ENTE-060120/513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0384		
treasury_and_risk_management_\(s4core\)					
Incorrect Authorization	17-12-2019	6.5	Transaction Management in SAP Treasury and Risk Management (corrected in S4CORE versions 1.01, 1.02, 1.03, 1.04 and EA-FINSERV versions 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2019-0383**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528880390	A-SAP-TREA-060120/514
Incorrect Authorization	17-12-2019	6.5	Transaction Management in SAP Treasury and Risk Management (corrected in S4CORE versions 1.01, 1.02, 1.03, 1.04 and EA-FINSERV versions 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0) does not perform necessary authorization checks for functionalities that require user identity. **CVE ID : CVE-2019-0384**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528880390	A-SAP-TREA-060120/515
shadow_project					
shadow					
Improper Privilege Management	18-12-2019	6.9	shadow 4.8, in certain circumstances affecting at least Gentoo, Arch Linux, and Void Linux, allows local users to obtain root access because setuid programs are misconfigured. Specifically, this affects shadow 4.8 when compiled using --with-libpam but without explicitly passing --disable-account-	N/A	A-SHA-SHAD-060120/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tools-setuid, and without a PAM configuration suitable for use with setuid account management tools. This combination leads to account management tools (groupadd, groupdel, groupmod, useradd, userdel, usermod) that can easily be used by unprivileged local users to escalate privileges to root in multiple ways. This issue became much more relevant in approximately December 2019 when an unrelated bug was fixed (i.e., the chmod calls to suidusbins were fixed in the upstream Makefile which is now included in the release version 4.8). **CVE ID : CVE-2019-19882**		
shadowsocks					
shadowsocks-libev					
Information Exposure	18-12-2019	5.8	An exploitable information disclosure vulnerability exists in the network packet handling functionality of Shadowsocks-libev 3.3.2. When utilizing a Stream Cipher, a specially crafted set of network packets can cause an outbound connection from the server, resulting in information disclosure. An attacker can send arbitrary packets to trigger this vulnerability.	N/A	A-SHA-SHAD-060120/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5152		
Solarwinds					
serv-u_ftp_server					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-12-2019	4	A CSV injection vulnerability exists in the web UI of SolarWinds Serv-U FTP Server v15.1.7. **CVE ID : CVE-2019-13181**	N/A	A-SOL-SERV-060120/518
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-12-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in the web UI of SolarWinds Serv-U FTP Server 15.1.7. **CVE ID : CVE-2019-13182**	N/A	A-SOL-SERV-060120/519
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	3.5	A cross-site scripting (XSS) vulnerability exists in SolarWinds Serv-U FTP Server 15.1.7 in the email parameter, a different vulnerability than CVE-2018-19934 and CVE-2019-13182. **CVE ID : CVE-2019-19829**	N/A	A-SOL-SERV-060120/520
Spip					
spip					
Improper Input Validation	17-12-2019	4	_core_/plugins/medias in SPIP 3.2.x before 3.2.7 allows remote authenticated authors to inject content into the database. **CVE ID : CVE-2019-19830**	N/A	A-SPI-SPIP-060120/521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sqlite					
sqlite					
NULL Pointer Dereference	18-12-2019	5	exprListAppendList in window.c in SQLite 3.30.1 allows attackers to trigger an invalid pointer dereference because constant integer values in ORDER BY clauses of window definitions are mishandled. **CVE ID : CVE-2019-19880**	N/A	A-SQL-SQLI-060120/522
statics-server_project					
statics-server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-12-2019	5	A path traversal in statics-server exists in all version that allows an attacker to perform a path traversal when a symlink is used within the working directory. **CVE ID : CVE-2019-15596**	N/A	A-STA-STAT-060120/523
sudo					
sudo					
N/A	19-12-2019	5	In Sudo through 1.8.29, an attacker with access to a Runas ALL sudoer account can impersonate a nonexistent user by invoking sudo with a numeric uid that is not associated with any user. **CVE ID : CVE-2019-19232**	https://www.sudo.ws/devel.html#1.8.30b2	A-SUD-SUDO-060120/524
N/A	19-12-2019	5	In Sudo through 1.8.29, the fact that a user has been blocked (e.g., by using the ! character in the shadow file instead of a password hash)	https://www.sudo.ws/devel.html#1.8.30b2	A-SUD-SUDO-060120/525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is not considered, allowing an attacker (who has access to a Runas ALL sudoer account) to impersonate any blocked user. **CVE ID : CVE-2019-19234**		
sylabs					
singularity					
Incorrect Default Permissions	18-12-2019	5	Insecure permissions (777) are set on $HOME/.singularity when it is newly created by Singularity (version from 3.3.0 to 3.5.1), which could lead to an information leak, and malicious redirection of operations performed against Sylabs cloud services. **CVE ID : CVE-2019-19724**	https://github.com/sylabs/singularity/releases/tag/v3.5.2	A-SYL-SING-060120/526
tautulli					
tautulli					
Cross-Site Request Forgery (CSRF)	18-12-2019	4.3	In Tautulli 2.1.9, CSRF in the /shutdown URI allows an attacker to shut down the remote media server. (Also, anonymous access can be achieved in applications that do not have a user login area). **CVE ID : CVE-2019-19833**	N/A	A-TAU-TAUT-060120/527
Tibco					
spotfire_analytics_platform_for_aws					
Incorrect Default Permissions	17-12-2019	6	The Visualizations component of TIBCO Software Inc.'s TIBCO Spotfire Analyst, TIBCO	N/A	A-TIB-SPOT-060120/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Deployment Kit, TIBCO Spotfire Desktop, and TIBCO Spotfire Desktop Language Packs contains a vulnerability that theoretically allows an attacker with permission to write DXP files to the Spotfire library to remotely execute code of their choice on the user account of other users who access the affected system. This attack is a risk only when the attacker has write access to a network file system shared with the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analyst: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0, TIBCO Spotfire Deployment Kit: versions 7.11.1 and below, TIBCO Spotfire Desktop: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, and TIBCO Spotfire Desktop Language Packs: versions 7.11.1 and below.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-17334		
Information Exposure	17-12-2019	4	The Data access layer component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains multiple vulnerabilities that theoretically allow an attacker access to data cached from a data source, or a portion of a data source, that the attacker should not have access to. The attacker would need privileges to save a Spotfire file to the library. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0. **CVE ID : CVE-2019-17335**	N/A	A-TIB-SPOT-060120/529
Insufficiently Protected Credentials	17-12-2019	4	The Data access layer component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains multiple vulnerabilities that theoretically allow an attacker access to	N/A	A-TIB-SPOT-060120/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information that can lead to obtaining credentials used to access Spotfire data sources. The attacker would need privileges to save a Spotfire file to the library, and only applies in a situation where NTLM credentials, or a credentials profile is in use. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0. **CVE ID : CVE-2019-17336**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-12-2019	4.3	The Spotfire library component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains a vulnerability that theoretically allows an attacker to perform a reflected cross-site scripting (XSS) attack. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0,	N/A	A-TIB-SPOT-060120/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0. **CVE ID : CVE-2019-17337**		
spotfire_server					
Information Exposure	17-12-2019	4	The Data access layer component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains multiple vulnerabilities that theoretically allow an attacker access to data cached from a data source, or a portion of a data source, that the attacker should not have access to. The attacker would need privileges to save a Spotfire file to the library. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0. **CVE ID : CVE-2019-17335**	N/A	A-TIB-SPOT-060120/532
Insufficiently Protected Credentials	17-12-2019	4	The Data access layer component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and	N/A	A-TIB-SPOT-060120/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TIBCO Spotfire Server contains multiple vulnerabilities that theoretically allow an attacker access to information that can lead to obtaining credentials used to access Spotfire data sources. The attacker would need privileges to save a Spotfire file to the library, and only applies in a situation where NTLM credentials, or a credentials profile is in use. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0. **CVE ID : CVE-2019-17336**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-12-2019	4.3	The Spotfire library component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains a vulnerability that theoretically allows an attacker to perform a reflected cross-site scripting (XSS) attack. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS	N/A	A-TIB-SPOT-060120/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marketplace: version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0. **CVE ID : CVE-2019-17337**		
spotfire_analyst					
Incorrect Default Permissions	17-12-2019	6	The Visualizations component of TIBCO Software Inc.'s TIBCO Spotfire Analyst, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Deployment Kit, TIBCO Spotfire Desktop, and TIBCO Spotfire Desktop Language Packs contains a vulnerability that theoretically allows an attacker with permission to write DXP files to the Spotfire library to remotely execute code of their choice on the user account of other users who access the affected system. This attack is a risk only when the attacker has write access to a network file system shared with the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analyst: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1,	N/A	A-TIB-SPOT-060120/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0, TIBCO Spotfire Deployment Kit: versions 7.11.1 and below, TIBCO Spotfire Desktop: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, and TIBCO Spotfire Desktop Language Packs: versions 7.11.1 and below. **CVE ID : CVE-2019-17334**		
spotfire_deployment_kit					
Incorrect Default Permissions	17-12-2019	6	The Visualizations component of TIBCO Software Inc.'s TIBCO Spotfire Analyst, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Deployment Kit, TIBCO Spotfire Desktop, and TIBCO Spotfire Desktop Language Packs contains a vulnerability that theoretically allows an attacker with permission to write DXP files to the Spotfire library to remotely execute code of their choice on the user account of other users who access the affected system. This attack is a risk only when the attacker has write access to a network file system shared	N/A	A-TIB-SPOT-060120/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analyst: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0, TIBCO Spotfire Deployment Kit: versions 7.11.1 and below, TIBCO Spotfire Desktop: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, and TIBCO Spotfire Desktop Language Packs: versions 7.11.1 and below. **CVE ID : CVE-2019-17334**		
spotfire_desktop					
Incorrect Default Permissions	17-12-2019	6	The Visualizations component of TIBCO Software Inc.'s TIBCO Spotfire Analyst, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Deployment Kit, TIBCO Spotfire Desktop, and TIBCO Spotfire Desktop Language Packs contains a vulnerability that theoretically allows an attacker with permission to write DXP files to the Spotfire library to remotely	N/A	A-TIB-SPOT-060120/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute code of their choice on the user account of other users who access the affected system. This attack is a risk only when the attacker has write access to a network file system shared with the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analyst: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0, TIBCO Spotfire Deployment Kit: versions 7.11.1 and below, TIBCO Spotfire Desktop: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, and TIBCO Spotfire Desktop Language Packs: versions 7.11.1 and below. **CVE ID : CVE-2019-17334**		
spotfire_desktop_language_packs					
Incorrect Default Permissions	17-12-2019	6	The Visualizations component of TIBCO Software Inc.'s TIBCO Spotfire Analyst, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Deployment Kit, TIBCO Spotfire Desktop, and	N/A	A-TIB-SPOT-060120/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TIBCO Spotfire Desktop Language Packs contains a vulnerability that theoretically allows an attacker with permission to write DXP files to the Spotfire library to remotely execute code of their choice on the user account of other users who access the affected system. This attack is a risk only when the attacker has write access to a network file system shared with the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analyst: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0, TIBCO Spotfire Deployment Kit: versions 7.11.1 and below, TIBCO Spotfire Desktop: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, and TIBCO Spotfire Desktop Language Packs: versions 7.11.1 and below. **CVE ID : CVE-2019-17334**		
Tigervnc					
tigervnc					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-12-2019	7.5	TigerVNC version prior to 1.10.1 is vulnerable to heap buffer overflow, which occurs in TightDecoder::FilterGradient. Exploitation of this vulnerability could potentially result into remote code execution. This attack appear to be exploitable via network connectivity. **CVE ID : CVE-2019-15693**	N/A	A-TIG-TIGE-060120/539
treekill_project					
treekill					
Improper Control of Generation of Code ('Code Injection')	18-12-2019	7.5	A Code Injection exists in treekill on Windows which allows a remote code execution when an attacker is able to control the input into the command. **CVE ID : CVE-2019-15598**	N/A	A-TRE-TREE-060120/540
tree-kill_project					
tree-kill					
Improper Control of Generation of Code ('Code Injection')	18-12-2019	7.5	A Code Injection exists in tree-kill on Windows which allows a remote code execution when an attacker is able to control the input into the command. **CVE ID : CVE-2019-15599**	N/A	A-TRE-TREE-060120/541
Trendmicro					
housecall_for_home_networks					
Improper Privilege Management	18-12-2019	4.4	A privilege escalation vulnerability in Trend Micro HouseCall for Home Networks (versions below	N/A	A-TRE-HOUS-060120/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.3.0.1063) could be exploited allowing an attacker to place a malicious DLL file into the application directory and elevate privileges. **CVE ID : CVE-2019-19688**		
Untrusted Search Path	18-12-2019	4.4	Trend Micro HouseCall for Home Networks (versions below 5.3.0.1063) could be exploited via a DLL Hijack related to a vulnerability on the packer that the program uses. **CVE ID : CVE-2019-19689**	N/A	A-TRE-HOUS-060120/543
mobile_security					
Weak Password Requirements	18-12-2019	7.5	Trend Micro Mobile Security for Android (Consumer) versions 10.3.1 and below on Android 8.0+ has an issue in which an attacker could bypass the product's App Password Protection feature. **CVE ID : CVE-2019-19690**	N/A	A-TRE-MOBI-060120/544
Typo3					
typo3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-12-2019	6.5	An issue was discovered in TYPO3 before 8.7.30, 9.x before 9.5.12, and 10.x before 10.2.2. It has been discovered that the extraction of manually uploaded ZIP archives in Extension Manager is vulnerable to directory traversal. Admin privileges are required in order to exploit this vulnerability. (In	N/A	A-TYP-TYPO-060120/545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v9 LTS and later, System Maintainer privileges are also required.) **CVE ID : CVE-2019-19848**		
Deserialization of Untrusted Data	17-12-2019	6.5	An issue was discovered in TYPO3 before 8.7.30, 9.x before 9.5.12, and 10.x before 10.2.2. It has been discovered that the classes QueryGenerator and QueryView are vulnerable to insecure deserialization. One exploitable scenario requires having the system extension ext:lowlevel (Backend Module: DB Check) installed, with a valid backend user who has administrator privileges. The other exploitable scenario requires having the system extension ext:sys_action installed, with a valid backend user who has limited privileges. **CVE ID : CVE-2019-19849**	N/A	A-TYP-TYPO-060120/546
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-12-2019	6.5	An issue was discovered in TYPO3 before 8.7.30, 9.x before 9.5.12, and 10.x before 10.2.2. Because escaping of user-submitted content is mishandled, the class QueryGenerator is vulnerable to SQL injection. Exploitation requires having the system extension ext:lowlevel installed, and a valid backend user who has administrator privileges. **CVE ID : CVE-2019-19850**	N/A	A-TYP-TYPO-060120/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
verot_project					
verot					
Unrestricted Upload of File with Dangerous Type	17-12-2019	7.5	class.upload.php in verot.net class.upload through 1.0.3 and 2.x through 2.0.4, as used in the K2 extension for Joomla! and other products, omits .pht from the set of dangerous file extensions, a similar issue to CVE-2019-19576. **CVE ID : CVE-2019-19634**	N/A	A-VER-VERO-060120/548
virglrenderer_project					
virglrenderer					
NULL Pointer Dereference	23-12-2019	2.1	A NULL pointer dereference in vrend_renderer.c in virglrenderer through 0.8.0 allows guest OS users to cause a denial of service via malformed commands. **CVE ID : CVE-2019-18388**	N/A	A-VIR-VIRG-060120/549
yarnpkg					
yarn					
Improper Link Resolution Before File Access ('Link Following')	16-12-2019	6.8	In Yarn before 1.21.1, the package install functionality can be abused to generate arbitrary symlinks on the host filesystem by using specially crafted "bin" keys. Existing files could be overwritten depending on the current user permission set. **CVE ID : CVE-2019-10773**	https://github.com/yarnpkg/yarn/issues/7761#issuecomment-565493023	A-YAR-YARN-060120/550
ZTE					
zxcloud_goldendata_vap					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure Through Log Files	23-12-2019	5	All versions up to V4.01.01.02 of ZTE ZXCLOUD GoldenData VAP product have a file reading vulnerability. Attackers could obtain log file information without authorization, causing the disclosure of sensitive information. **CVE ID : CVE-2019-3429**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1012023	A-ZTE-ZXCL-060120/551
Information Exposure	23-12-2019	4	All versions up to V4.01.01.02 of ZTE ZXCLOUD GoldenData VAP product have an information disclosure vulnerability. Attackers could use this vulnerability to collect data information and damage the system. **CVE ID : CVE-2019-3430**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1012023	A-ZTE-ZXCL-060120/552
Insufficiently Protected Credentials	23-12-2019	5	All versions up to V4.01.01.02 of ZTE ZXCLOUD GoldenData VAP product have encryption problems vulnerability. Attackers could sniff unencrypted account and password through the network for front-end system access. **CVE ID : CVE-2019-3431**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1012023	A-ZTE-ZXCL-060120/553
Zulip					
zulip_server					
URL Redirection to Untrusted Site ('Open	18-12-2019	5.8	The image thumbnailing handler in Zulip Server versions 1.9.0 to before 2.0.8 allowed an open redirect that was visible to logged-in	https://blog.zulip.org/2019/12/13/zulip-server-2-0-	A-ZUL-ZULI-060120/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redirect')			users. **CVE ID : CVE-2019-19775**	8-security-release/, https://github.com/zulip/zulip/commit/b7c87a4d82397a5e6ac169b6098bed0b1ae7a583	
Operating System					
Advantech					
diaganywhere_server_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-12-2019	7.5	In Advantech DiagAnywhere Server, Versions 3.07.11 and prior, multiple stack-based buffer overflow vulnerabilities exist in the file transfer service listening on the TCP port. Successful exploitation could allow an unauthenticated attacker to execute arbitrary code with the privileges of the user running DiagAnywhere Server. **CVE ID : CVE-2019-18257**	N/A	O-ADV-DIAG-060120/555
Apple					
mac_os					
Improper Privilege Management	19-12-2019	7.5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a binary planting (default folder privilege escalation)	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2019-16444**		
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16445**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/557
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16446**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/558
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution . **CVE ID : CVE-2019-16448**		
Information Exposure	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16449**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/560
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16450**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/561
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16451		
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16452**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/563
Improper Input Validation	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a security bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-16453**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/564
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16454**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16455**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/566
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16456**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/567
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16457**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16458**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/569
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16459**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/570
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16460**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/571
Out-of-	19-12-2019	5	Adobe Acrobat and Reader	https://hel	O-APP-MAC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16461**	px.adobe.com/security/products/acrobat/apsb19-55.html	060120/572
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16462**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/573
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16463**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/574
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056	https://helpx.adobe.co	O-APP-MAC_-060120/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16464**	m/security /products/ acrobat/aps b19-55.html	
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16465**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-APP-MAC_-060120/576
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-12-2019	9.3	Adobe Photoshop CC versions before 20.0.8 and 21.0.x before 21.0.2 have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8253**	https://helpx.adobe.com/security/products/photoshop/apsb19-56.html	O-APP-MAC_-060120/577
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-12-2019	9.3	Adobe Photoshop CC versions before 20.0.8 and 21.0.x before 21.0.2 have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8254**	https://helpx.adobe.com/security/products/photoshop/apsb19-56.html	O-APP-MAC_-060120/578

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
iphone_os					
Information Exposure	18-12-2019	2.1	The issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 13. A person with physical access to an iOS device may be able to access contacts from the lock screen. **CVE ID : CVE-2019-8742**	N/A	O-APP-IPHO-060120/579
Improper Authenticati on	18-12-2019	4.6	This issue was addressed by improving Face ID machine learning models. This issue is fixed in iOS 13. A 3D model constructed to look like the enrolled user may authenticate via Face ID. **CVE ID : CVE-2019-8760**	N/A	O-APP-IPHO-060120/580
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.1 and iPadOS 13.1, tvOS 13, Safari 13.0.1, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8763**	N/A	O-APP-IPHO-060120/581
Information Exposure	18-12-2019	4.3	An issue existed in the drawing of web page elements. The issue was addressed with improved logic. This issue is fixed in iOS 13.1 and iPadOS 13.1, macOS Catalina 10.15. Visiting a maliciously crafted	N/A	O-APP-IPHO-060120/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			website may reveal browsing history. **CVE ID : CVE-2019-8769**		
Information Exposure	18-12-2019	2.1	The issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 13.1 and iPadOS 13.1. A person with physical access to an iOS device may be able to access contacts from the lock screen. **CVE ID : CVE-2019-8775**	N/A	O-APP-IPHO-060120/583
Exposure of Resource to Wrong Sphere	18-12-2019	7.5	A logic issue applied the incorrect restrictions. This issue was addressed by updating the logic to apply the correct restrictions. This issue is fixed in iOS 13.1.1 and iPadOS 13.1.1. Third party app extensions may not receive the correct sandbox restrictions. **CVE ID : CVE-2019-8779**	N/A	O-APP-IPHO-060120/584
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8782**	N/A	O-APP-IPHO-060120/585
Improper Restriction of	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling.	N/A	O-APP-IPHO-060120/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8783**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8784**	N/A	O-APP-IPHO-060120/587
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8785**	N/A	O-APP-IPHO-060120/588
Improper Restriction of Operations within the	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS	N/A	O-APP-IPHO-060120/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8786**		
Out-of-bounds Read	18-12-2019	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8787**	N/A	O-APP-IPHO-060120/590
Improper Input Validation	18-12-2019	5	An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1. Improper URL processing may lead to data exfiltration. **CVE ID : CVE-2019-8788**	N/A	O-APP-IPHO-060120/591
Improper Link Resolution Before File Access ('Link Following')	18-12-2019	4.3	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1. Parsing a maliciously crafted iBooks file may lead to disclosure of user information. **CVE ID : CVE-2019-8789**	N/A	O-APP-IPHO-060120/592
Improper Neutralizatio	18-12-2019	6.8	An injection issue was addressed with improved	N/A	O-APP-IPHO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements in Output Used by a Downstream Component ('Injection')			validation. This issue is fixed in Shazam Android App Version 9.25.0, Shazam iOS App Version 12.11.0. Processing a maliciously crafted URL may lead to arbitrary javascript code execution. **CVE ID : CVE-2019-8792**		060120/593
Improper Input Validation	18-12-2019	2.1	A consistency issue existed in deciding when to show the screen recording indicator. The issue was resolved with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2. A local user may be able to record the screen without a visible screen recording indicator. **CVE ID : CVE-2019-8793**	N/A	O-APP-IPHO-060120/594
Improper Input Validation	18-12-2019	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to read restricted memory. **CVE ID : CVE-2019-8794**	N/A	O-APP-IPHO-060120/595
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2. An application may be able to execute arbitrary code with system privileges.	N/A	O-APP-IPHO-060120/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8795		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8797**	N/A	O-APP-IPHO-060120/597
Out-of-bounds Read	18-12-2019	2.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-6207**	N/A	O-APP-IPHO-060120/598
Incorrect Permission Assignment for Critical Resource	18-12-2019	4.3	A consistency issue was addressed with improved state handling. This issue is fixed in iOS 12.2. A website may be able to access the microphone without the microphone use indicator being shown. **CVE ID : CVE-2019-6222**	N/A	O-APP-IPHO-060120/599
Improper Restriction of Operations within the Bounds of a	18-12-2019	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.4. An application may be able to execute arbitrary	N/A	O-APP-IPHO-060120/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			code with kernel privileges. **CVE ID : CVE-2019-7287**		
Out-of-bounds Read	18-12-2019	2.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-8510**	N/A	O-APP-IPHO-060120/601
Improper Privilege Management	18-12-2019	6.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8514**	N/A	O-APP-IPHO-060120/602
Improper Input Validation	18-12-2019	5	A validation issue was addressed with improved logic. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. Processing a maliciously crafted string may lead to a denial of service. **CVE ID : CVE-2019-8516**	N/A	O-APP-IPHO-060120/603
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11.	N/A	O-APP-IPHO-060120/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8523**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	9.4	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2019-8527**	N/A	O-APP-IPHO-060120/605
Out-of-bounds Write	18-12-2019	7.2	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8529**	N/A	O-APP-IPHO-060120/606
Improper Input Validation	18-12-2019	5.8	This issue was addressed with improved checks. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2. A malicious application may be able to overwrite arbitrary files. **CVE ID : CVE-2019-8530**	N/A	O-APP-IPHO-060120/607
Improper Restriction of Operations within the Bounds of a	18-12-2019	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for	N/A	O-APP-IPHO-060120/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8535**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8536**	N/A	O-APP-IPHO-060120/609
Improper Initialization	18-12-2019	7.1	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-8540**	N/A	O-APP-IPHO-060120/610
N/A	18-12-2019	2.1	A privacy issue existed in motion sensor calibration. This issue was addressed with improved motion sensor processing. This issue is fixed in iOS 12.2, watchOS 5.2. A malicious app may be able to track users between installs. **CVE ID : CVE-2019-8541**	N/A	O-APP-IPHO-060120/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8542**	N/A	O-APP-IPHO-060120/612
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8544**	N/A	O-APP-IPHO-060120/613
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.6	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A local user may be able to cause unexpected system termination or read kernel memory. **CVE ID : CVE-2019-8545**	N/A	O-APP-IPHO-060120/614
Information Exposure	18-12-2019	2.1	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 12.2,	N/A	O-APP-IPHO-060120/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			macOS Mojave 10.14.4, watchOS 5.2. A local user may be able to view sensitive user information. **CVE ID : CVE-2019-8546**		
Improper Input Validation	18-12-2019	9.3	Multiple input validation issues existed in MIG generated code. These issues were addressed with improved validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8549**	N/A	O-APP-IPHO-060120/616
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8551**	N/A	O-APP-IPHO-060120/617
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8552**	N/A	O-APP-IPHO-060120/618
Improper Restriction	18-12-2019	6.8	A memory corruption issue was addressed with	N/A	O-APP-IPHO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2. Clicking a malicious SMS link may lead to arbitrary code execution. **CVE ID : CVE-2019-8553**		060120/619
Incorrect Permission Assignment for Critical Resource	18-12-2019	4.3	A permissions issue existed in the handling of motion and orientation data. This issue was addressed with improved restrictions. This issue is fixed in iOS 12.2. A website may be able to access sensor information without user consent. **CVE ID : CVE-2019-8554**	N/A	O-APP-IPHO-060120/620
Use After Free	18-12-2019	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8556**	N/A	O-APP-IPHO-060120/621
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to	N/A	O-APP-IPHO-060120/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2019-8558**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8559**	N/A	O-APP-IPHO-060120/623
Out-of-bounds Read	18-12-2019	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to read restricted memory. **CVE ID : CVE-2019-8560**	N/A	O-APP-IPHO-060120/624
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2019-8562**	N/A	O-APP-IPHO-060120/625
Improper Restriction of Operations within the Bounds of a	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for	N/A	O-APP-IPHO-060120/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8563**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-12-2019	7.6	A race condition was addressed with additional validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4. A malicious application may be able to gain root privileges. **CVE ID : CVE-2019-8565**	N/A	O-APP-IPHO-060120/627
Information Exposure	18-12-2019	4.3	An API issue existed in the handling of microphone data. This issue was addressed with improved validation. This issue is fixed in iOS 12.2. A malicious application may be able to access the microphone without indication to the user. **CVE ID : CVE-2019-8566**	N/A	O-APP-IPHO-060120/628
Information Exposure	18-12-2019	5	A user privacy issue was addressed by removing the broadcast MAC address. This issue is fixed in iOS 12.2. A device may be passively tracked by its WiFi MAC address. **CVE ID : CVE-2019-8567**	N/A	O-APP-IPHO-060120/629
Improper Link Resolution Before File Access ('Link	18-12-2019	2.1	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed	N/A	O-APP-IPHO-060120/630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Following')			in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to modify protected parts of the file system. **CVE ID : CVE-2019-8568**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8571**	N/A	O-APP-IPHO-060120/631
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8574**	N/A	O-APP-IPHO-060120/632
Out-of-bounds Read	18-12-2019	6.6	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to cause unexpected system termination or read kernel memory.	N/A	O-APP-IPHO-060120/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8576		
Improper Input Validation	18-12-2019	6.8	An input validation issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8577**	N/A	O-APP-IPHO-060120/634
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8583**	N/A	O-APP-IPHO-060120/635
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8584**	N/A	O-APP-IPHO-060120/636
Out-of-	18-12-2019	6.8	An out-of-bounds read was	N/A	O-APP-IPHO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. Processing a maliciously crafted movie file may lead to arbitrary code execution. **CVE ID : CVE-2019-8585**		060120/637
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8586**	N/A	O-APP-IPHO-060120/638
Improper Validation of Array Index	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8587**	N/A	O-APP-IPHO-060120/639
Access of Resource Using Incompatible	18-12-2019	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS	N/A	O-APP-IPHO-060120/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type ('Type Confusion')			Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. An application may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2019-8591**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8593**	N/A	O-APP-IPHO-060120/641
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8594**	N/A	O-APP-IPHO-060120/642
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may	N/A	O-APP-IPHO-060120/643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2019-8595**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8596**	N/A	O-APP-IPHO-060120/644
Access of Resource Using Incompatible Type ('Type Confusion')	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8597**	N/A	O-APP-IPHO-060120/645
Improper Input Validation	18-12-2019	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to read restricted	N/A	O-APP-IPHO-060120/646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory. **CVE ID : CVE-2019-8598**		
Information Exposure	18-12-2019	2.1	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 12.3. A person with physical access to an iOS device may be able to see the email address used for iTunes. **CVE ID : CVE-2019-8599**	N/A	O-APP-IPHO-060120/647
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A maliciously crafted SQL query may lead to arbitrary code execution. **CVE ID : CVE-2019-8600**	N/A	O-APP-IPHO-060120/648
Integer Overflow or Wraparound	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8601**	N/A	O-APP-IPHO-060120/649
Improper Restriction of Operations	18-12-2019	6.8	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 12.3,	N/A	O-APP-IPHO-060120/650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8602**		
Use After Free	18-12-2019	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8605**	N/A	O-APP-IPHO-060120/651
Out-of-bounds Read	18-12-2019	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may result in the disclosure of process memory. **CVE ID : CVE-2019-8607**	N/A	O-APP-IPHO-060120/652
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously	N/A	O-APP-IPHO-060120/653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8608**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8609**	N/A	O-APP-IPHO-060120/654
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8610**	N/A	O-APP-IPHO-060120/655
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously	N/A	O-APP-IPHO-060120/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8611**		
Use After Free	18-12-2019	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2019-8613**	N/A	O-APP-IPHO-060120/657
Out-of-bounds Read	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8615**	N/A	O-APP-IPHO-060120/658
Improper Input Validation	18-12-2019	6.8	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 12.3. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2019-8617**	N/A	O-APP-IPHO-060120/659
Improper Restriction of Operations within the	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5,	N/A	O-APP-IPHO-060120/660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8619**		
Information Exposure	18-12-2019	5	A user privacy issue was addressed by removing the broadcast MAC address. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A device may be passively tracked by its WiFi MAC address. **CVE ID : CVE-2019-8620**	N/A	O-APP-IPHO-060120/661
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8622**	N/A	O-APP-IPHO-060120/662
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing	N/A	O-APP-IPHO-060120/663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8623**		
Improper Input Validation	18-12-2019	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, watchOS 5.2.1. Processing a maliciously crafted message may lead to a denial of service. **CVE ID : CVE-2019-8626**	N/A	O-APP-IPHO-060120/664
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8628**	N/A	O-APP-IPHO-060120/665
N/A	18-12-2019	2.1	The issue was addressed with improved UI handling. This issue is fixed in iOS 12.3. The lock screen may show a locked icon after unlocking. **CVE ID : CVE-2019-8630**	N/A	O-APP-IPHO-060120/666
Improper Input Validation	18-12-2019	9.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A malicious	N/A	O-APP-IPHO-060120/667

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application may be able to gain root privileges. **CVE ID : CVE-2019-8637**		
Out-of-bounds Read	18-12-2019	7.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8641**	N/A	O-APP-IPHO-060120/668
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8644**	N/A	O-APP-IPHO-060120/669
Out-of-bounds Read	18-12-2019	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8646**	N/A	O-APP-IPHO-060120/670
Use After	18-12-2019	7.5	A use after free issue was addressed with improved	N/A	O-APP-IPHO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			memory management. This issue is fixed in iOS 12.4, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2019-8647**		060120/671
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2019-8648**	N/A	O-APP-IPHO-060120/672
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of synchronous page loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8649**	N/A	O-APP-IPHO-060120/673
Out-of-bounds Read	18-12-2019	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. Parsing a maliciously crafted office	N/A	O-APP-IPHO-060120/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			document may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8657**		
Out-of-bounds Read	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8658**	N/A	O-APP-IPHO-060120/675
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8660**	N/A	O-APP-IPHO-060120/676
Use After Free	18-12-2019	7.5	This issue was addressed with improved checks. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. An attacker may be able to trigger a use-after-free in an application deserializing an untrusted NSDictionary.	N/A	O-APP-IPHO-060120/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8662		
Information Exposure	18-12-2019	5	This issue was addressed with improved checks. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8663**	N/A	O-APP-IPHO-060120/678
Improper Input Validation	18-12-2019	5	A denial of service issue was addressed with improved validation. This issue is fixed in iOS 12.4, watchOS 5.3. A remote attacker may cause an unexpected application termination. **CVE ID : CVE-2019-8665**	N/A	O-APP-IPHO-060120/679
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8666**	N/A	O-APP-IPHO-060120/680
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for	N/A	O-APP-IPHO-060120/681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8669**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8671**	N/A	O-APP-IPHO-060120/682
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8672**	N/A	O-APP-IPHO-060120/683
Improper Restriction of Operations within the Bounds of a	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2,	N/A	O-APP-IPHO-060120/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8673**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13, Safari 13. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8674**	N/A	O-APP-IPHO-060120/685
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8676**	N/A	O-APP-IPHO-060120/686
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13,	N/A	O-APP-IPHO-060120/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8677**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8678**	N/A	O-APP-IPHO-060120/688
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8679**	N/A	O-APP-IPHO-060120/689
Improper Restriction of Operations within the	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6,	N/A	O-APP-IPHO-060120/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8680**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8681**	N/A	O-APP-IPHO-060120/691
Missing Authenticati on for Critical Function	18-12-2019	2.1	The issue was addressed with improved UI handling. This issue is fixed in iOS 12.4, watchOS 5.3. A user may inadvertently complete an in-app purchase while on the lock screen. **CVE ID : CVE-2019-8682**	N/A	O-APP-IPHO-060120/692
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for	N/A	O-APP-IPHO-060120/693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8683**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8684**	N/A	O-APP-IPHO-060120/694
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8685**	N/A	O-APP-IPHO-060120/695
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6,	N/A	O-APP-IPHO-060120/696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8686**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8687**	N/A	O-APP-IPHO-060120/697
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8688**	N/A	O-APP-IPHO-060120/698
Improper Restriction	18-12-2019	9.3	Multiple memory corruption issues were addressed with	N/A	O-APP-IPHO-060120/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8689**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of document loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8690**	N/A	O-APP-IPHO-060120/700
Improper Input Validation	18-12-2019	4.3	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in iOS 12.4, tvOS 12.4. A malicious application may be able to restrict access to websites. **CVE ID : CVE-2019-8698**	N/A	O-APP-IPHO-060120/701
Improper Input	18-12-2019	5	A logic issue existed in the handling of answering phone	N/A	O-APP-IPHO-060120/702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			calls. The issue was addressed with improved state management. This issue is fixed in iOS 12.4. The initiator of a phone call may be able to cause the recipient to answer a simultaneous Walkie-Talkie connection. **CVE ID : CVE-2019-8699**		
Improper Authenticati on	18-12-2019	2.1	An authentication issue was addressed with improved state management. This issue is fixed in tvOS 13. A local user may be able to leak sensitive user information. **CVE ID : CVE-2019-8704**	N/A	O-APP-IPHO-060120/703
Information Exposure	18-12-2019	5	A logic issue existed with the display of notification previews. This issue was addressed with improved validation. This issue is fixed in iOS 13. Notification previews may show on Bluetooth accessories even when previews are disabled. **CVE ID : CVE-2019-8711**	N/A	O-APP-IPHO-060120/704
Improper Input Validation	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2019-8727**	N/A	O-APP-IPHO-060120/705
Incorrect Default Permissions	18-12-2019	4.3	A permissions issue existed in which execute permission was incorrectly granted. This issue was addressed with improved permission	N/A	O-APP-IPHO-060120/706

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation. This issue is fixed in iOS 13. Processing a maliciously crafted file may disclose user information. **CVE ID : CVE-2019-8731**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	2.1	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8798**	N/A	O-APP-IPHO-060120/707
Insufficient Session Expiration	18-12-2019	4.6	An authentication issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A local attacker may be able to login to the account of a previously logged in user without valid credentials.. **CVE ID : CVE-2019-8803**	N/A	O-APP-IPHO-060120/708
Improper Authenticati on	18-12-2019	2.9	An inconsistency in Wi-Fi network configuration settings was addressed. This issue is fixed in iOS 13.2 and iPadOS 13.2. An attacker in physical proximity may be able to force a user onto a malicious Wi-Fi network during device setup. **CVE ID : CVE-2019-8804**	N/A	O-APP-IPHO-060120/709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8808**	N/A	O-APP-IPHO-060120/710
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8811**	N/A	O-APP-IPHO-060120/711
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8812**	N/A	O-APP-IPHO-060120/712
Improper	18-12-2019	4.3	A logic issue was addressed	N/A	O-APP-IPHO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8813**		060120/713
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8814**	N/A	O-APP-IPHO-060120/714
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8815**	N/A	O-APP-IPHO-060120/715
Improper Restriction	18-12-2019	9.3	Multiple memory corruption issues were addressed with	N/A	O-APP-IPHO-060120/716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8816**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8819**	N/A	O-APP-IPHO-060120/717
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8820**	N/A	O-APP-IPHO-060120/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8821**	N/A	O-APP-IPHO-060120/719
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8822**	N/A	O-APP-IPHO-060120/720
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8823**	N/A	O-APP-IPHO-060120/721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mac_os_x					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	This issue was addressed with improved handling of file metadata. This issue is fixed in macOS Mojave 10.14.4. A malicious application may bypass Gatekeeper checks. **CVE ID : CVE-2019-6239**	N/A	O-APP-MAC_-060120/722
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15, tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2019-8745**	N/A	O-APP-MAC_-060120/723
NULL Pointer Dereference	18-12-2019	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8748**	N/A	O-APP-MAC_-060120/724
NULL Pointer Dereference	18-12-2019	7.2	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-8755**	N/A	O-APP-MAC_-060120/725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-12-2019	1.9	A race condition existed when reading and writing user preferences. This was addressed with improved state handling. This issue is fixed in macOS Catalina 10.15. The "Share Mac Analytics" setting may not be disabled when a user deselects the switch to share analytics. **CVE ID : CVE-2019-8757**	N/A	O-APP-MAC_-060120/726
NULL Pointer Dereference	18-12-2019	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8758**	N/A	O-APP-MAC_-060120/727
Information Exposure	18-12-2019	5	"Clear History and Website Data" did not clear the history. The issue was addressed with improved data deletion. This issue is fixed in macOS Catalina 10.15. A user may be unable to delete browsing history items. **CVE ID : CVE-2019-8768**	N/A	O-APP-MAC_-060120/728
Information Exposure	18-12-2019	4.3	An issue existed in the drawing of web page elements. The issue was addressed with improved logic. This issue is fixed in iOS 13.1 and iPadOS 13.1, macOS Catalina 10.15. Visiting a maliciously crafted	N/A	O-APP-MAC_-060120/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			website may reveal browsing history. **CVE ID : CVE-2019-8769**		
Incorrect Permission Assignment for Critical Resource	18-12-2019	4.3	The issue was addressed with improved permissions logic. This issue is fixed in macOS Catalina 10.15. A malicious application may be able to access recent documents. **CVE ID : CVE-2019-8770**	N/A	O-APP-MAC_-060120/730
Inadequate Encryption Strength	18-12-2019	5	An issue existed in the handling of links in encrypted PDFs. This issue was addressed by adding a confirmation prompt. This issue is fixed in macOS Catalina 10.15. An attacker may be able to exfiltrate the contents of an encrypted PDF. **CVE ID : CVE-2019-8772**	N/A	O-APP-MAC_-060120/731
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8781**	N/A	O-APP-MAC_-060120/732
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for	N/A	O-APP-MAC_-060120/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Windows 7.15. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8784**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8785**	N/A	O-APP-MAC_-060120/734
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8786**	N/A	O-APP-MAC_-060120/735
Out-of-bounds Read	18-12-2019	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8787**	N/A	O-APP-MAC_-060120/736
Improper Input	18-12-2019	5	An issue existed in the parsing of URLs. This issue was addressed with	N/A	O-APP-MAC_-060120/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			improved input validation. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1. Improper URL processing may lead to data exfiltration. **CVE ID : CVE-2019-8788**		
Improper Link Resolution Before File Access ('Link Following')	18-12-2019	4.3	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1. Parsing a maliciously crafted iBooks file may lead to disclosure of user information. **CVE ID : CVE-2019-8789**	N/A	O-APP-MAC_-060120/738
Improper Input Validation	18-12-2019	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to read restricted memory. **CVE ID : CVE-2019-8794**	N/A	O-APP-MAC_-060120/739
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges.	N/A	O-APP-MAC_-060120/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8797		
Out-of-bounds Read	18-12-2019	2.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-6207**	N/A	O-APP-MAC_-060120/741
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-12-2019	10	Brackets versions 1.14 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8255**	https://helpx.adobe.com/security/products/brackets/apsb19-57.html	O-APP-MAC_-060120/742
Improper Input Validation	18-12-2019	2.1	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Mojave 10.14.4. Processing malicious data may lead to unexpected application termination. **CVE ID : CVE-2019-8507**	N/A	O-APP-MAC_-060120/743
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Mojave 10.14.4. Mounting a maliciously crafted NFS network share may lead to arbitrary code execution	N/A	O-APP-MAC_-060120/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with system privileges. **CVE ID : CVE-2019-8508**		
Out-of-bounds Read	18-12-2019	2.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-8510**	N/A	O-APP-MAC_-060120/745
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-12-2019	7.2	This issue was addressed with improved checks. This issue is fixed in macOS Mojave 10.14.4. A local user may be able to execute arbitrary shell commands. **CVE ID : CVE-2019-8513**	N/A	O-APP-MAC_-060120/746
Improper Privilege Management	18-12-2019	6.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8514**	N/A	O-APP-MAC_-060120/747
Improper Input Validation	18-12-2019	5	A validation issue was addressed with improved logic. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. Processing a maliciously crafted string may lead to a	N/A	O-APP-MAC_-060120/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service. **CVE ID : CVE-2019-8516**		
Out-of-bounds Read	18-12-2019	2.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Mojave 10.14.4. An application may be able to read restricted memory. **CVE ID : CVE-2019-8519**	N/A	O-APP-MAC_-060120/749
Out-of-bounds Read	18-12-2019	2.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Mojave 10.14.4. A malicious application may be able to read restricted memory. **CVE ID : CVE-2019-8520**	N/A	O-APP-MAC_-060120/750
Insufficiently Protected Credentials	18-12-2019	2.1	A logic issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.4. An encrypted volume may be unmounted and remounted by a different user without prompting for the password. **CVE ID : CVE-2019-8522**	N/A	O-APP-MAC_-060120/751
Use After Free	18-12-2019	7.2	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Mojave 10.14.4. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8526**	N/A	O-APP-MAC_-060120/752
Buffer Copy without	18-12-2019	9.4	A buffer overflow was addressed with improved	N/A	O-APP-MAC_-060120/753

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			size validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2019-8527**		
Out-of-bounds Write	18-12-2019	7.2	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8529**	N/A	O-APP-MAC_-060120/754
Improper Input Validation	18-12-2019	5.8	This issue was addressed with improved checks. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2. A malicious application may be able to overwrite arbitrary files. **CVE ID : CVE-2019-8530**	N/A	O-APP-MAC_-060120/755
Improper Authentication	18-12-2019	4.6	A lock handling issue was addressed with improved lock handling. This issue is fixed in macOS Mojave 10.14.4. A Mac may not lock when disconnecting from an external monitor. **CVE ID : CVE-2019-8533**	N/A	O-APP-MAC_-060120/756
Information Exposure	18-12-2019	2.1	An access issue was addressed with improved memory management. This issue is fixed in macOS Mojave 10.14.4. A local user	N/A	O-APP-MAC_-060120/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may be able to view a user?s locked notes. **CVE ID : CVE-2019-8537**		
Improper Initialization	18-12-2019	7.1	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-8540**	N/A	O-APP-MAC_-060120/758
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8542**	N/A	O-APP-MAC_-060120/759
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.6	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A local user may be able to cause unexpected system termination or read kernel memory. **CVE ID : CVE-2019-8545**	N/A	O-APP-MAC_-060120/760
Information Exposure	18-12-2019	2.1	An access issue was addressed with additional sandbox restrictions. This	N/A	O-APP-MAC_-060120/761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in iOS 12.2, macOS Mojave 10.14.4, watchOS 5.2. A local user may be able to view sensitive user information. **CVE ID : CVE-2019-8546**		
Improper Input Validation	18-12-2019	9.3	Multiple input validation issues existed in MIG generated code. These issues were addressed with improved validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8549**	N/A	O-APP-MAC_-060120/762
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8552**	N/A	O-APP-MAC_-060120/763
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Mojave 10.14.4. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8555**	N/A	O-APP-MAC_-060120/764
Out-of-bounds Read	18-12-2019	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue	N/A	O-APP-MAC_-060120/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to read restricted memory. **CVE ID : CVE-2019-8560**		
Improper Input Validation	18-12-2019	6.8	A logic issue was addressed with improved validation. This issue is fixed in macOS Mojave 10.14.4. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8561**	N/A	O-APP-MAC_-060120/766
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-12-2019	7.6	A race condition was addressed with additional validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4. A malicious application may be able to gain root privileges. **CVE ID : CVE-2019-8565**	N/A	O-APP-MAC_-060120/767
Improper Link Resolution Before File Access ('Link Following')	18-12-2019	2.1	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to modify protected parts of the file system. **CVE ID : CVE-2019-8568**	N/A	O-APP-MAC_-060120/768
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1,	N/A	O-APP-MAC_-060120/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8571**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8574**	N/A	O-APP-MAC_-060120/770
Out-of-bounds Read	18-12-2019	6.6	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to cause unexpected system termination or read kernel memory. **CVE ID : CVE-2019-8576**	N/A	O-APP-MAC_-060120/771
Improper Input Validation	18-12-2019	6.8	An input validation issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8577**	N/A	O-APP-MAC_-060120/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8583**	N/A	O-APP-MAC_-060120/773
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8584**	N/A	O-APP-MAC_-060120/774
Out-of-bounds Read	18-12-2019	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. Processing a maliciously crafted movie file may lead to arbitrary code execution. **CVE ID : CVE-2019-8585**	N/A	O-APP-MAC_-060120/775
Improper Restriction of	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling.	N/A	O-APP-MAC_-060120/776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8586**		
Improper Validation of Array Index	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8587**	N/A	O-APP-MAC_-060120/777
Improper Input Validation	18-12-2019	4.3	This issue was addressed with improved checks. This issue is fixed in macOS Mojave 10.14.5. A malicious application may bypass Gatekeeper checks. **CVE ID : CVE-2019-8589**	N/A	O-APP-MAC_-060120/778
Improper Input Validation	18-12-2019	9.3	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8590**	N/A	O-APP-MAC_-060120/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	18-12-2019	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. An application may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2019-8591**	N/A	O-APP-MAC_-060120/780
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8594**	N/A	O-APP-MAC_-060120/781
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8595**	N/A	O-APP-MAC_-060120/782
Improper Restriction	18-12-2019	6.8	Multiple memory corruption issues were addressed with	N/A	O-APP-MAC_-060120/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8596**		
Access of Resource Using Incompatible Type ('Type Confusion')	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8597**	N/A	O-APP-MAC_-060120/784
Improper Input Validation	18-12-2019	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to read restricted memory. **CVE ID : CVE-2019-8598**	N/A	O-APP-MAC_-060120/785
Improper Neutralizatio n of Special	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation.	N/A	O-APP-MAC_-060120/786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A maliciously crafted SQL query may lead to arbitrary code execution. **CVE ID : CVE-2019-8600**		
Integer Overflow or Wraparound	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8601**	N/A	O-APP-MAC_-060120/787
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8602**	N/A	O-APP-MAC_-060120/788
Out-of-bounds Read	18-12-2019	6.8	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.5. An application may be able to read restricted	N/A	O-APP-MAC_-060120/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory. **CVE ID : CVE-2019-8603**		
Out-of-bounds Write	18-12-2019	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8604**	N/A	O-APP-MAC_-060120/790
Use After Free	18-12-2019	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8605**	N/A	O-APP-MAC_-060120/791
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-12-2019	6.9	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Mojave 10.14.5. A local user may be able to load unsigned kernel extensions. **CVE ID : CVE-2019-8606**	N/A	O-APP-MAC_-060120/792
Out-of-bounds Read	18-12-2019	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12.	N/A	O-APP-MAC_-060120/793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may result in the disclosure of process memory. **CVE ID : CVE-2019-8607**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8608**	N/A	O-APP-MAC_-060120/794
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8609**	N/A	O-APP-MAC_-060120/795
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12.	N/A	O-APP-MAC_-060120/796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8610**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8611**	N/A	O-APP-MAC_-060120/797
Out-of-bounds Read	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8615**	N/A	O-APP-MAC_-060120/798
NULL Pointer Dereference	18-12-2019	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges.	N/A	O-APP-MAC_-060120/799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8616		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8619**	N/A	O-APP-MAC_-060120/800
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8622**	N/A	O-APP-MAC_-060120/801
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	O-APP-MAC_-060120/802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8623		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8628**	N/A	O-APP-MAC_-060120/803
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8629**	N/A	O-APP-MAC_-060120/804
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.5	An authentication issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.5. A user may be unexpectedly logged in to another user?s account. **CVE ID : CVE-2019-8634**	N/A	O-APP-MAC_-060120/805
Double Free	18-12-2019	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges.	N/A	O-APP-MAC_-060120/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8635		
Out-of-bounds Read	18-12-2019	7.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8641**	N/A	O-APP-MAC_-060120/807
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8644**	N/A	O-APP-MAC_-060120/808
Out-of-bounds Read	18-12-2019	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8646**	N/A	O-APP-MAC_-060120/809
Improper Restriction of Operations	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS	N/A	O-APP-MAC_-060120/810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2019-8648**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of synchronous page loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8649**	N/A	O-APP-MAC_-060120/811
Out-of-bounds Read	18-12-2019	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. Parsing a maliciously crafted office document may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8657**	N/A	O-APP-MAC_-060120/812
Out-of-bounds Read	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2,	N/A	O-APP-MAC_-060120/813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8658**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8660**	N/A	O-APP-MAC_-060120/814
Use After Free	18-12-2019	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Mojave 10.14.6. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2019-8661**	N/A	O-APP-MAC_-060120/815
Use After Free	18-12-2019	7.5	This issue was addressed with improved checks. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. An attacker may be able to trigger a use-after-free in an application deserializing an untrusted NSDictionary. **CVE ID : CVE-2019-8662**	N/A	O-APP-MAC_-060120/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	18-12-2019	5	This issue was addressed with improved checks. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8663**	N/A	O-APP-MAC_-060120/817
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8666**	N/A	O-APP-MAC_-060120/818
Improper Input Validation	18-12-2019	5	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.6. The encryption status of a Time Machine backup may be incorrect. **CVE ID : CVE-2019-8667**	N/A	O-APP-MAC_-060120/819
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for	N/A	O-APP-MAC_-060120/820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8669**		
Improper Input Validation	18-12-2019	4.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.6, Safari 12.1.2. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2019-8670**	N/A	O-APP-MAC_-060120/821
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8671**	N/A	O-APP-MAC_-060120/822
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for	N/A	O-APP-MAC_-060120/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8672**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8673**	N/A	O-APP-MAC_-060120/824
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8676**	N/A	O-APP-MAC_-060120/825
Improper Restriction of Operations within the Bounds of a	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2,	N/A	O-APP-MAC_-060120/826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8677**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8678**	N/A	O-APP-MAC_-060120/827
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8679**	N/A	O-APP-MAC_-060120/828
Improper Restriction of	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling.	N/A	O-APP-MAC_-060120/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8680**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8681**	N/A	O-APP-MAC_-060120/830
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8683**	N/A	O-APP-MAC_-060120/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8684**	N/A	O-APP-MAC_-060120/832
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8685**	N/A	O-APP-MAC_-060120/833
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code	N/A	O-APP-MAC_-060120/834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2019-8686**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8687**	N/A	O-APP-MAC_-060120/835
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8688**	N/A	O-APP-MAC_-060120/836
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for	N/A	O-APP-MAC_-060120/837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8689**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of document loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8690**	N/A	O-APP-MAC_-060120/838
Improper Input Validation	18-12-2019	2.1	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.6. An application may be able to read restricted memory. **CVE ID : CVE-2019-8691**	N/A	O-APP-MAC_-060120/839
Out-of-bounds Read	18-12-2019	2.1	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.6. An application may be able to read restricted memory. **CVE ID : CVE-2019-8692**	N/A	O-APP-MAC_-060120/840
Out-of-bounds Read	18-12-2019	4.3	A validation issue was addressed with improved input sanitization. This issue	N/A	O-APP-MAC_-060120/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is fixed in macOS Mojave 10.14.6. An application may be able to read restricted memory. **CVE ID : CVE-2019-8693**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8694**	N/A	O-APP-MAC_-060120/842
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8695**	N/A	O-APP-MAC_-060120/843
Out-of-bounds Write	18-12-2019	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8697**	N/A	O-APP-MAC_-060120/844
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with	N/A	O-APP-MAC_-060120/845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			system privileges. **CVE ID : CVE-2019-8701**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.3	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15, tvOS 13. Processing a maliciously crafted movie may result in the disclosure of process memory. **CVE ID : CVE-2019-8705**	N/A	O-APP-MAC_-060120/846
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15, tvOS 13. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8717**	N/A	O-APP-MAC_-060120/847
Information Exposure	18-12-2019	2.1	The contents of locked notes sometimes appeared in search results. This issue was addressed with improved data cleanup. This issue is fixed in macOS Catalina 10.15. A local user may be able to view a user?s locked notes. **CVE ID : CVE-2019-8730**	N/A	O-APP-MAC_-060120/848
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	2.1	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute	N/A	O-APP-MAC_-060120/849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			arbitrary code with system privileges. **CVE ID : CVE-2019-8798**		
Untrusted Search Path	18-12-2019	4.4	A dynamic library loading issue existed in iTunes setup. This was addressed with improved path searching. This issue is fixed in macOS Catalina 10.15.1, iTunes for Windows 12.10.2. Running the iTunes installer in an untrusted directory may result in arbitrary code execution. **CVE ID : CVE-2019-8801**	N/A	O-APP-MAC_-060120/850
Improper Input Validation	18-12-2019	9.3	A validation issue was addressed with improved logic. This issue is fixed in macOS Catalina 10.15.1. A malicious application may be able to gain root privileges. **CVE ID : CVE-2019-8802**	N/A	O-APP-MAC_-060120/851
Insufficient Session Expiration	18-12-2019	4.6	An authentication issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A local attacker may be able to login to the account of a previously logged in user without valid credentials.. **CVE ID : CVE-2019-8803**	N/A	O-APP-MAC_-060120/852
Improper Input Validation	18-12-2019	9.3	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This	N/A	O-APP-MAC_-060120/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in macOS Catalina 10.15.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8805**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8807**	N/A	O-APP-MAC_-060120/854
Improper Input Validation	18-12-2019	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Catalina 10.15.1. An application may be able to read restricted memory. **CVE ID : CVE-2019-8817**	N/A	O-APP-MAC_-060120/855
watchos					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8743**	N/A	O-APP-WATC-060120/856
Improper Restriction of Operations within the	18-12-2019	9.3	A memory corruption vulnerability was addressed with improved locking. This issue is fixed in watchOS 6.1. An application may be able	N/A	O-APP-WATC-060120/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8747**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in watchOS 6.1, iCloud for Windows 11.0. Multiple issues in libxslt. **CVE ID : CVE-2019-8750**	N/A	O-APP-WATC-060120/858
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8764**	N/A	O-APP-WATC-060120/859
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8765**	N/A	O-APP-WATC-060120/860
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	O-APP-WATC-060120/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8766		
Information Exposure	18-12-2019	2.1	The issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 13.1 and iPadOS 13.1. A person with physical access to an iOS device may be able to access contacts from the lock screen. **CVE ID : CVE-2019-8775**	N/A	O-APP-WATC-060120/862
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8785**	N/A	O-APP-WATC-060120/863
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8786**	N/A	O-APP-WATC-060120/864
Out-of-bounds Read	18-12-2019	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS	N/A	O-APP-WATC-060120/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.1. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8787**		
Improper Input Validation	18-12-2019	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to read restricted memory. **CVE ID : CVE-2019-8794**	N/A	O-APP-WATC-060120/866
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8797**	N/A	O-APP-WATC-060120/867
Out-of-bounds Read	18-12-2019	2.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-6207**	N/A	O-APP-WATC-060120/868
Out-of-bounds Read	18-12-2019	2.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory.	N/A	O-APP-WATC-060120/869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-8510**		
Improper Privilege Management	18-12-2019	6.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8514**	N/A	O-APP-WATC-060120/870
Improper Input Validation	18-12-2019	5	A validation issue was addressed with improved logic. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. Processing a maliciously crafted string may lead to a denial of service. **CVE ID : CVE-2019-8516**	N/A	O-APP-WATC-060120/871
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	9.4	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2019-8527**	N/A	O-APP-WATC-060120/872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8536**	N/A	O-APP-WATC-060120/873
Improper Initialization	18-12-2019	7.1	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-8540**	N/A	O-APP-WATC-060120/874
N/A	18-12-2019	2.1	A privacy issue existed in motion sensor calibration. This issue was addressed with improved motion sensor processing. This issue is fixed in iOS 12.2, watchOS 5.2. A malicious app may be able to track users between installs. **CVE ID : CVE-2019-8541**	N/A	O-APP-WATC-060120/875
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2, iTunes 12.9.4 for Windows, iCloud for	N/A	O-APP-WATC-060120/876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 7.11. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8544**	N/A	O-APP-WATC-060120/877
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.6	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A local user may be able to cause unexpected system termination or read kernel memory. **CVE ID : CVE-2019-8545**	N/A	O-APP-WATC-060120/878
Information Exposure	18-12-2019	2.1	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, watchOS 5.2. A local user may be able to view sensitive user information. **CVE ID : CVE-2019-8546**	N/A	O-APP-WATC-060120/879
Information	18-12-2019	2.1	An issue existed where partially entered passcodes	N/A	O-APP-WATC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			may not clear when the device went to sleep. This issue was addressed by clearing the passcode when a locked device sleeps. This issue is fixed in watchOS 5.2. A partially entered passcode may not clear when the device goes to sleep. **CVE ID : CVE-2019-8548**		060120/880
Improper Input Validation	18-12-2019	9.3	Multiple input validation issues existed in MIG generated code. These issues were addressed with improved validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8549**	N/A	O-APP-WATC-060120/881
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8552**	N/A	O-APP-WATC-060120/882
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2. Clicking a malicious SMS link may lead to arbitrary code execution.	N/A	O-APP-WATC-060120/883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8553		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8558**	N/A	O-APP-WATC-060120/884
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8559**	N/A	O-APP-WATC-060120/885
Out-of-bounds Read	18-12-2019	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to read restricted memory. **CVE ID : CVE-2019-8560**	N/A	O-APP-WATC-060120/886
Improper Restriction of Operations within the	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2,	N/A	O-APP-WATC-060120/887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8563**		
Improper Link Resolution Before File Access ('Link Following')	18-12-2019	2.1	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to modify protected parts of the file system. **CVE ID : CVE-2019-8568**	N/A	O-APP-WATC-060120/888
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8574**	N/A	O-APP-WATC-060120/889
Out-of-bounds Read	18-12-2019	6.6	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to cause unexpected system termination or read kernel memory. **CVE ID : CVE-2019-8576**	N/A	O-APP-WATC-060120/890

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-12-2019	6.8	An input validation issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8577**	N/A	O-APP-WATC-060120/891
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8583**	N/A	O-APP-WATC-060120/892
Out-of-bounds Read	18-12-2019	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. Processing a maliciously crafted movie file may lead to arbitrary code execution. **CVE ID : CVE-2019-8585**	N/A	O-APP-WATC-060120/893
Access of Resource Using Incompatible Type ('Type	18-12-2019	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3,	N/A	O-APP-WATC-060120/894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Confusion')			watchOS 5.2.1. An application may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2019-8591**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8593**	N/A	O-APP-WATC-060120/895
Access of Resource Using Incompatible Type ('Type Confusion')	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8597**	N/A	O-APP-WATC-060120/896
Improper Input Validation	18-12-2019	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to read restricted memory.	N/A	O-APP-WATC-060120/897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8598		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A maliciously crafted SQL query may lead to arbitrary code execution. **CVE ID : CVE-2019-8600**	N/A	O-APP-WATC-060120/898
Integer Overflow or Wraparound	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8601**	N/A	O-APP-WATC-060120/899
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8602**	N/A	O-APP-WATC-060120/900
Use After Free	18-12-2019	9.3	A use after free issue was addressed with improved	N/A	O-APP-WATC-060120/901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory management. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8605**		
Out-of-bounds Read	18-12-2019	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may result in the disclosure of process memory. **CVE ID : CVE-2019-8607**	N/A	O-APP-WATC-060120/902
Use After Free	18-12-2019	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2019-8613**	N/A	O-APP-WATC-060120/903
Information Exposure	18-12-2019	5	A user privacy issue was addressed by removing the broadcast MAC address. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A device may be passively tracked by its WiFi MAC address. **CVE ID : CVE-2019-8620**	N/A	O-APP-WATC-060120/904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8622**	N/A	O-APP-WATC-060120/905
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8623**	N/A	O-APP-WATC-060120/906
Out-of-bounds Read	18-12-2019	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 5.3. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8624**	N/A	O-APP-WATC-060120/907
Improper Input Validation	18-12-2019	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, watchOS 5.2.1. Processing a maliciously	N/A	O-APP-WATC-060120/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted message may lead to a denial of service. **CVE ID : CVE-2019-8626**		
Improper Input Validation	18-12-2019	9.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to gain root privileges. **CVE ID : CVE-2019-8637**	N/A	O-APP-WATC-060120/909
Out-of-bounds Read	18-12-2019	7.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8641**	N/A	O-APP-WATC-060120/910
Out-of-bounds Read	18-12-2019	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8646**	N/A	O-APP-WATC-060120/911
Use After Free	18-12-2019	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.4, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause arbitrary code	N/A	O-APP-WATC-060120/912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2019-8647**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2019-8648**	N/A	O-APP-WATC-060120/913
Out-of-bounds Read	18-12-2019	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. Parsing a maliciously crafted office document may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8657**	N/A	O-APP-WATC-060120/914
Out-of-bounds Read	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8658**	N/A	O-APP-WATC-060120/915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-12-2019	5	This issue was addressed with improved checks. This issue is fixed in watchOS 5.3. Users removed from an iMessage conversation may still be able to alter state. **CVE ID : CVE-2019-8659**	N/A	O-APP-WATC-060120/916
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8660**	N/A	O-APP-WATC-060120/917
Use After Free	18-12-2019	7.5	This issue was addressed with improved checks. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. An attacker may be able to trigger a use-after-free in an application deserializing an untrusted NSDictionary. **CVE ID : CVE-2019-8662**	N/A	O-APP-WATC-060120/918
Improper Input Validation	18-12-2019	5	A denial of service issue was addressed with improved validation. This issue is fixed in iOS 12.4, watchOS 5.3. A remote attacker may cause an unexpected application termination. **CVE ID : CVE-2019-8665**	N/A	O-APP-WATC-060120/919
Improper Restriction of	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling.	N/A	O-APP-WATC-060120/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8669**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8672**	N/A	O-APP-WATC-060120/921
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8676**	N/A	O-APP-WATC-060120/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authenticati on for Critical Function	18-12-2019	2.1	The issue was addressed with improved UI handling. This issue is fixed in iOS 12.4, watchOS 5.3. A user may inadvertently complete an in-app purchase while on the lock screen. **CVE ID : CVE-2019-8682**	N/A	O-APP-WATC-060120/923
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8683**	N/A	O-APP-WATC-060120/924
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8684**	N/A	O-APP-WATC-060120/925
Improper Restriction of	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling.	N/A	O-APP-WATC-060120/926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8685**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8688**	N/A	O-APP-WATC-060120/927
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8689**	N/A	O-APP-WATC-060120/928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	2.1	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8798**	N/A	O-APP-WATC-060120/929
Insufficient Session Expiration	18-12-2019	4.6	An authentication issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A local attacker may be able to login to the account of a previously logged in user without valid credentials.. **CVE ID : CVE-2019-8803**	N/A	O-APP-WATC-060120/930
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8808**	N/A	O-APP-WATC-060120/931
Improper Restriction of Operations	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2	N/A	O-APP-WATC-060120/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8811**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8812**	N/A	O-APP-WATC-060120/933
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8816**	N/A	O-APP-WATC-060120/934
Improper Restriction of	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling.	N/A	O-APP-WATC-060120/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8820**		
tvos					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15, tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing a maliciously crafted text file may lead to arbitrary code execution. **CVE ID : CVE-2019-8745**	N/A	O-APP-TVOS-060120/936
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.1 and iPadOS 13.1, tvOS 13, Safari 13.0.1, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8763**	N/A	O-APP-TVOS-060120/937
Improper Restriction	18-12-2019	6.8	Multiple memory corruption issues were addressed with	N/A	O-APP-TVOS-060120/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8782**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8783**	N/A	O-APP-TVOS-060120/939
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8785**	N/A	O-APP-TVOS-060120/940
Improper Restriction of Operations within the	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS	N/A	O-APP-TVOS-060120/941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8786**		
Out-of-bounds Read	18-12-2019	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8787**	N/A	O-APP-TVOS-060120/942
Improper Input Validation	18-12-2019	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to read restricted memory. **CVE ID : CVE-2019-8794**	N/A	O-APP-TVOS-060120/943
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8795**	N/A	O-APP-TVOS-060120/944
Improper Restriction of Operations within the	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS	N/A	O-APP-TVOS-060120/945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8797**		
Out-of-bounds Read	18-12-2019	2.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-6207**	N/A	O-APP-TVOS-060120/946
Out-of-bounds Read	18-12-2019	2.1	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-8510**	N/A	O-APP-TVOS-060120/947
Improper Privilege Management	18-12-2019	6.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8514**	N/A	O-APP-TVOS-060120/948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-12-2019	5	A validation issue was addressed with improved logic. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. Processing a maliciously crafted string may lead to a denial of service. **CVE ID : CVE-2019-8516**	N/A	O-APP-TVOS-060120/949
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8523**	N/A	O-APP-TVOS-060120/950
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	9.4	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2019-8527**	N/A	O-APP-TVOS-060120/951
Improper Input Validation	18-12-2019	5.8	This issue was addressed with improved checks. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2. A malicious application may be able to overwrite arbitrary files.	N/A	O-APP-TVOS-060120/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8530		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8535**	N/A	O-APP-TVOS-060120/953
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8536**	N/A	O-APP-TVOS-060120/954
Improper Initialization	18-12-2019	7.1	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2019-8540**	N/A	O-APP-TVOS-060120/955
Buffer Copy without Checking Size of Input	18-12-2019	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 12.2, macOS	N/A	O-APP-TVOS-060120/956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Mojave 10.14.4, tvOS 12.2, watchOS 5.2, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8544**	N/A	O-APP-TVOS-060120/957
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.6	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A local user may be able to cause unexpected system termination or read kernel memory. **CVE ID : CVE-2019-8545**	N/A	O-APP-TVOS-060120/958
Improper Input Validation	18-12-2019	9.3	Multiple input validation issues existed in MIG generated code. These issues were addressed with improved validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A	N/A	O-APP-TVOS-060120/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8549**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8551**	N/A	O-APP-TVOS-060120/960
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8552**	N/A	O-APP-TVOS-060120/961
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2. Clicking a malicious SMS link may lead to arbitrary code execution. **CVE ID : CVE-2019-8553**	N/A	O-APP-TVOS-060120/962
Use After Free	18-12-2019	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud	N/A	O-APP-TVOS-060120/963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8556**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8558**	N/A	O-APP-TVOS-060120/964
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8559**	N/A	O-APP-TVOS-060120/965
Out-of-bounds Read	18-12-2019	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to read restricted memory. **CVE ID : CVE-2019-8560**	N/A	O-APP-TVOS-060120/966

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2019-8562**	N/A	O-APP-TVOS-060120/967
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8563**	N/A	O-APP-TVOS-060120/968
Improper Link Resolution Before File Access ('Link Following')	18-12-2019	2.1	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to modify protected parts of the file system. **CVE ID : CVE-2019-8568**	N/A	O-APP-TVOS-060120/969
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1,	N/A	O-APP-TVOS-060120/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8571**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8574**	N/A	O-APP-TVOS-060120/971
Out-of-bounds Read	18-12-2019	6.6	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to cause unexpected system termination or read kernel memory. **CVE ID : CVE-2019-8576**	N/A	O-APP-TVOS-060120/972
Improper Input Validation	18-12-2019	6.8	An input validation issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. An application may be able to gain elevated privileges. **CVE ID : CVE-2019-8577**	N/A	O-APP-TVOS-060120/973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8583**	N/A	O-APP-TVOS-060120/974
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8584**	N/A	O-APP-TVOS-060120/975
Out-of-bounds Read	18-12-2019	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. Processing a maliciously crafted movie file may lead to arbitrary code execution. **CVE ID : CVE-2019-8585**	N/A	O-APP-TVOS-060120/976
Improper Restriction of	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling.	N/A	O-APP-TVOS-060120/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8586**		
Improper Validation of Array Index	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8587**	N/A	O-APP-TVOS-060120/978
Access of Resource Using Incompatible Type ('Type Confusion')	18-12-2019	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. An application may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2019-8591**	N/A	O-APP-TVOS-060120/979
Improper Restriction of Operations within the	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS	N/A	O-APP-TVOS-060120/980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			5.2.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8593**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8594**	N/A	O-APP-TVOS-060120/981
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8595**	N/A	O-APP-TVOS-060120/982
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously	N/A	O-APP-TVOS-060120/983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8596**		
Access of Resource Using Incompatible Type ('Type Confusion')	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8597**	N/A	O-APP-TVOS-060120/984
Improper Input Validation	18-12-2019	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to read restricted memory. **CVE ID : CVE-2019-8598**	N/A	O-APP-TVOS-060120/985
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A maliciously crafted SQL query may lead to arbitrary	N/A	O-APP-TVOS-060120/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution. **CVE ID : CVE-2019-8600**		
Integer Overflow or Wraparound	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8601**	N/A	O-APP-TVOS-060120/987
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-8602**	N/A	O-APP-TVOS-060120/988
Use After Free	18-12-2019	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8605**	N/A	O-APP-TVOS-060120/989
Out-of-bounds Read	18-12-2019	4.3	An out-of-bounds read was addressed with improved input validation. This issue is	N/A	O-APP-TVOS-060120/990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may result in the disclosure of process memory. **CVE ID : CVE-2019-8607**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8608**	N/A	O-APP-TVOS-060120/991
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8609**	N/A	O-APP-TVOS-060120/992
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling.	N/A	O-APP-TVOS-060120/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8610**		
Use After Free	18-12-2019	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2019-8613**	N/A	O-APP-TVOS-060120/994
Out-of-bounds Read	18-12-2019	4.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8615**	N/A	O-APP-TVOS-060120/995
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5,	N/A	O-APP-TVOS-060120/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8619**		
Information Exposure	18-12-2019	5	A user privacy issue was addressed by removing the broadcast MAC address. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A device may be passively tracked by its WiFi MAC address. **CVE ID : CVE-2019-8620**	N/A	O-APP-TVOS-060120/997
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8622**	N/A	O-APP-TVOS-060120/998
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to	N/A	O-APP-TVOS-060120/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2019-8623**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8625**	N/A	O-APP-TVOS-060120/1000
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8628**	N/A	O-APP-TVOS-060120/1001
Improper Input Validation	18-12-2019	9.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to gain root privileges. **CVE ID : CVE-2019-8637**	N/A	O-APP-TVOS-060120/1002
Out-of-bounds Read	18-12-2019	7.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS	N/A	O-APP-TVOS-060120/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8641**		
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8644**	N/A	O-APP-TVOS-060120/1004
Out-of-bounds Read	18-12-2019	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8646**	N/A	O-APP-TVOS-060120/1005
Use After Free	18-12-2019	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.4, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2019-8647**	N/A	O-APP-TVOS-060120/1006

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2019-8648**	N/A	O-APP-TVOS-060120/1007
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of synchronous page loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8649**	N/A	O-APP-TVOS-060120/1008
Out-of-bounds Read	18-12-2019	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. Parsing a maliciously crafted office document may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8657**	N/A	O-APP-TVOS-060120/1009
Out-of-bounds Read	18-12-2019	4.3	A logic issue was addressed with improved state	N/A	O-APP-TVOS-060120/1010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8658**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2019-8660**	N/A	O-APP-TVOS-060120/1011
Use After Free	18-12-2019	7.5	This issue was addressed with improved checks. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. An attacker may be able to trigger a use-after-free in an application deserializing an untrusted NSDictionary. **CVE ID : CVE-2019-8662**	N/A	O-APP-TVOS-060120/1012
Improper Restriction of Operations within the Bounds of a	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2,	N/A	O-APP-TVOS-060120/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8666**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8669**	N/A	O-APP-TVOS-060120/1014
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8671**	N/A	O-APP-TVOS-060120/1015
Improper Restriction of	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling.	N/A	O-APP-TVOS-060120/1016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8672**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8673**	N/A	O-APP-TVOS-060120/1017
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8676**	N/A	O-APP-TVOS-060120/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8677**	N/A	O-APP-TVOS-060120/1019
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8678**	N/A	O-APP-TVOS-060120/1020
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code	N/A	O-APP-TVOS-060120/1021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2019-8679**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8680**	N/A	O-APP-TVOS-060120/1022
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8681**	N/A	O-APP-TVOS-060120/1023
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for	N/A	O-APP-TVOS-060120/1024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8683**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8684**	N/A	O-APP-TVOS-060120/1025
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8685**	N/A	O-APP-TVOS-060120/1026
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2,	N/A	O-APP-TVOS-060120/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8686**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8687**	N/A	O-APP-TVOS-060120/1028
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8688**	N/A	O-APP-TVOS-060120/1029
Improper Restriction of	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling.	N/A	O-APP-TVOS-060120/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8689**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue existed in the handling of document loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8690**	N/A	O-APP-TVOS-060120/1031
Improper Input Validation	18-12-2019	4.3	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in iOS 12.4, tvOS 12.4. A malicious application may be able to restrict access to websites. **CVE ID : CVE-2019-8698**	N/A	O-APP-TVOS-060120/1032
Improper Authentication	18-12-2019	2.1	An authentication issue was addressed with improved state management. This	N/A	O-APP-TVOS-060120/1033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in tvOS 13. A local user may be able to leak sensitive user information. **CVE ID : CVE-2019-8704**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.3	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15, tvOS 13. Processing a maliciously crafted movie may result in the disclosure of process memory. **CVE ID : CVE-2019-8705**	N/A	O-APP-TVOS-060120/1034
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8707**	N/A	O-APP-TVOS-060120/1035
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15, tvOS 13. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8717**	N/A	O-APP-TVOS-060120/1036
Improper Neutralizatio n of Input	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is	N/A	O-APP-TVOS-060120/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8719**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8726**	N/A	O-APP-TVOS-060120/1038
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8733**	N/A	O-APP-TVOS-060120/1039
Use After Free	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14.	N/A	O-APP-TVOS-060120/1040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8735**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	2.1	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8798**	N/A	O-APP-TVOS-060120/1041
Insufficient Session Expiration	18-12-2019	4.6	An authentication issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A local attacker may be able to login to the account of a previously logged in user without valid credentials.. **CVE ID : CVE-2019-8803**	N/A	O-APP-TVOS-060120/1042
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	O-APP-TVOS-060120/1043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8808		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8811**	N/A	O-APP-TVOS-060120/1044
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8812**	N/A	O-APP-TVOS-060120/1045
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8813**	N/A	O-APP-TVOS-060120/1046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8814**	N/A	O-APP-TVOS-060120/1047
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8815**	N/A	O-APP-TVOS-060120/1048
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	O-APP-TVOS-060120/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8816		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8819**	N/A	O-APP-TVOS-060120/1050
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8820**	N/A	O-APP-TVOS-060120/1051
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to	N/A	O-APP-TVOS-060120/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2019-8821**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8822**	N/A	O-APP-TVOS-060120/1053
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8823**	N/A	O-APP-TVOS-060120/1054
ipados					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.1 and iPadOS 13.1, tvOS 13, Safari 13.0.1, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web	N/A	O-APP-IPAD-060120/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			content may lead to arbitrary code execution. **CVE ID : CVE-2019-8763**		
Information Exposure	18-12-2019	4.3	An issue existed in the drawing of web page elements. The issue was addressed with improved logic. This issue is fixed in iOS 13.1 and iPadOS 13.1, macOS Catalina 10.15. Visiting a maliciously crafted website may reveal browsing history. **CVE ID : CVE-2019-8769**	N/A	O-APP-IPAD-060120/1056
Information Exposure	18-12-2019	2.1	The issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 13.1 and iPadOS 13.1. A person with physical access to an iOS device may be able to access contacts from the lock screen. **CVE ID : CVE-2019-8775**	N/A	O-APP-IPAD-060120/1057
Exposure of Resource to Wrong Sphere	18-12-2019	7.5	A logic issue applied the incorrect restrictions. This issue was addressed by updating the logic to apply the correct restrictions. This issue is fixed in iOS 13.1.1 and iPadOS 13.1.1. Third party app extensions may not receive the correct sandbox restrictions. **CVE ID : CVE-2019-8779**	N/A	O-APP-IPAD-060120/1058
Improper Restriction of Operations	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2	N/A	O-APP-IPAD-060120/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8782**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8783**	N/A	O-APP-IPAD-060120/1060
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8784**	N/A	O-APP-IPAD-060120/1061
Improper Restriction of Operations within the	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS	N/A	O-APP-IPAD-060120/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8785**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2019-8786**	N/A	O-APP-IPAD-060120/1063
Out-of-bounds Read	18-12-2019	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A remote attacker may be able to leak memory. **CVE ID : CVE-2019-8787**	N/A	O-APP-IPAD-060120/1064
Improper Input Validation	18-12-2019	5	An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1. Improper URL processing may lead to data exfiltration. **CVE ID : CVE-2019-8788**	N/A	O-APP-IPAD-060120/1065
Improper Link Resolution	18-12-2019	4.3	A validation issue existed in the handling of symlinks. This issue was addressed	N/A	O-APP-IPAD-060120/1066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Before File Access ('Link Following')			with improved validation of symlinks. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1. Parsing a maliciously crafted iBooks file may lead to disclosure of user information. **CVE ID : CVE-2019-8789**		
Improper Input Validation	18-12-2019	2.1	A consistency issue existed in deciding when to show the screen recording indicator. The issue was resolved with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2. A local user may be able to record the screen without a visible screen recording indicator. **CVE ID : CVE-2019-8793**	N/A	O-APP-IPAD-060120/1067
Improper Input Validation	18-12-2019	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to read restricted memory. **CVE ID : CVE-2019-8794**	N/A	O-APP-IPAD-060120/1068
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2. An application may be able to execute arbitrary code with system privileges.	N/A	O-APP-IPAD-060120/1069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8795		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8797**	N/A	O-APP-IPAD-060120/1070
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	2.1	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2019-8798**	N/A	O-APP-IPAD-060120/1071
Insufficient Session Expiration	18-12-2019	4.6	An authentication issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A local attacker may be able to login to the account of a previously logged in user without valid credentials.. **CVE ID : CVE-2019-8803**	N/A	O-APP-IPAD-060120/1072
Improper Authenticati on	18-12-2019	2.9	An inconsistency in Wi-Fi network configuration settings was addressed. This issue is fixed in iOS 13.2 and	N/A	O-APP-IPAD-060120/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 13.2. An attacker in physical proximity may be able to force a user onto a malicious Wi-Fi network during device setup. **CVE ID : CVE-2019-8804**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8808**	N/A	O-APP-IPAD-060120/1074
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8811**	N/A	O-APP-IPAD-060120/1075
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2.	N/A	O-APP-IPAD-060120/1076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8812**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2019-8813**	N/A	O-APP-IPAD-060120/1077
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8814**	N/A	O-APP-IPAD-060120/1078
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing	N/A	O-APP-IPAD-060120/1079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8815**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8816**	N/A	O-APP-IPAD-060120/1080
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8819**	N/A	O-APP-IPAD-060120/1081
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0,	N/A	O-APP-IPAD-060120/1082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8820**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8821**	N/A	O-APP-IPAD-060120/1083
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8822**	N/A	O-APP-IPAD-060120/1084
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for	N/A	O-APP-IPAD-060120/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-8823**		
Barco					
clickshare_button_r9861500d01_firmware					
Insufficiently Protected Credentials	17-12-2019	6.8	Barco ClickShare Button R9861500D01 devices before 1.9.0 have incorrect Credentials Management. The ClickShare Button implements encryption at rest which uses a one-time programmable (OTP) AES encryption key. This key is shared across all ClickShare Buttons of model R9861500D01. **CVE ID : CVE-2019-18832**	N/A	O-BAR-CLIC-060120/1086
Missing Encryption of Sensitive Data	17-12-2019	4.3	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information exposure (issue 2 of 2).. The encryption key of the media content which is shared between a ClickShare Button and a ClickShare Base Unit is randomly generated for each new session and communicated over a TLS connection. An attacker who is able to perform a Man-in-the-Middle attack between the TLS connection, is able to obtain the encryption key. **CVE ID : CVE-2019-18833**	N/A	O-BAR-CLIC-060120/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-12-2019	6.9	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Missing Support for Integrity Check. The ClickShare Button does not verify the integrity of the mutable content on the UBIFS partition before being used. **CVE ID : CVE-2019-18824**	N/A	O-BAR-CLIC-060120/1088
Untrusted Search Path	17-12-2019	4.4	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Missing Support for Integrity Check. The Barco signed 'Clickshare_For_Windows.exe' binary on the ClickShare Button (R9861500D01) loads a number of DLL files dynamically without verifying their integrity. **CVE ID : CVE-2019-18829**	N/A	O-BAR-CLIC-060120/1089
clickshare_cs-100_huddle_firmware					
N/A	17-12-2019	5	Barco ClickShare Huddle CS-100 devices before 1.9.0 and CSE-200 devices before 1.9.0 have incorrect Credentials Management. The ClickShare Base Unit implements encryption at rest using encryption keys which are shared across all ClickShare Base Units of models CS-100 & CSE-200. **CVE ID : CVE-2019-18825**	N/A	O-BAR-CLIC-060120/1090
clickshare_cse-200_firmware					
Improper Neutralization of Special	16-12-2019	10	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow OS	N/A	O-BAR-CLIC-060120/1091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			Command Injection. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, is vulnerable to OS command injection vulnerabilities. These vulnerabilities could lead to code execution on the ClickShare Button with the privileges of the user 'nobody'. **CVE ID : CVE-2019-18830**		
Information Exposure	16-12-2019	3.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information Exposure. The encrypted ClickShare Button firmware contains the private key of a test device-certificate. **CVE ID : CVE-2019-18831**	N/A	O-BAR-CLIC-060120/1092
N/A	17-12-2019	5	Barco ClickShare Huddle CS-100 devices before 1.9.0 and CSE-200 devices before 1.9.0 have incorrect Credentials Management. The ClickShare Base Unit implements encryption at rest using encryption keys which are shared across all ClickShare Base Units of models CS-100 & CSE-200. **CVE ID : CVE-2019-18825**	N/A	O-BAR-CLIC-060120/1093
Improper Certificate Validation	16-12-2019	7.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Improper Following of a Certificate's	N/A	O-BAR-CLIC-060120/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Chain of Trust. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, does not properly validate the whole certificate chain. **CVE ID : CVE-2019-18826**		
Improper Input Validation	16-12-2019	4.3	On Barco ClickShare Button R9861500D01 devices (before firmware version 1.9.0) JTAG access is disabled after ROM code execution. This means that JTAG access is possible when the system is running code from ROM before handing control over to embedded firmware. **CVE ID : CVE-2019-18827**	N/A	O-BAR-CLIC-060120/1095
Insufficiently Protected Credentials	16-12-2019	7.2	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Insufficiently Protected Credentials. The root account (present for access via debug interfaces, which are by default not enabled on production devices) of the embedded Linux on the ClickShare Button is using a weak password. **CVE ID : CVE-2019-18828**	N/A	O-BAR-CLIC-060120/1096
clickshare_cs-100_firmware					
Improper Neutralization of Special Elements	16-12-2019	10	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow OS Command Injection. The	N/A	O-BAR-CLIC-060120/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, is vulnerable to OS command injection vulnerabilities. These vulnerabilities could lead to code execution on the ClickShare Button with the privileges of the user 'nobody'. **CVE ID : CVE-2019-18830**		
Information Exposure	16-12-2019	3.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information Exposure. The encrypted ClickShare Button firmware contains the private key of a test device-certificate. **CVE ID : CVE-2019-18831**	N/A	O-BAR-CLIC-060120/1098
Improper Certificate Validation	16-12-2019	7.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Improper Following of a Certificate's Chain of Trust. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, does not properly validate the whole certificate chain. **CVE ID : CVE-2019-18826**	N/A	O-BAR-CLIC-060120/1099
Improper Input Validation	16-12-2019	4.3	On Barco ClickShare Button R9861500D01 devices (before firmware version 1.9.0) JTAG access is	N/A	O-BAR-CLIC-060120/1100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disabled after ROM code execution. This means that JTAG access is possible when the system is running code from ROM before handing control over to embedded firmware. **CVE ID : CVE-2019-18827**		
Insufficiently Protected Credentials	16-12-2019	7.2	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Insufficiently Protected Credentials. The root account (present for access via debug interfaces, which are by default not enabled on production devices) of the embedded Linux on the ClickShare Button is using a weak password. **CVE ID : CVE-2019-18828**	N/A	O-BAR-CLIC-060120/1101
clickshare_cse-200\+_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-12-2019	10	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow OS Command Injection. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, is vulnerable to OS command injection vulnerabilities. These vulnerabilities could lead to code execution on the ClickShare Button with the privileges of the user 'nobody'. **CVE ID : CVE-2019-18830**	N/A	O-BAR-CLIC-060120/1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	16-12-2019	3.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information Exposure. The encrypted ClickShare Button firmware contains the private key of a test device-certificate. **CVE ID : CVE-2019-18831**	N/A	O-BAR-CLIC-060120/1103
Improper Certificate Validation	16-12-2019	7.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Improper Following of a Certificate's Chain of Trust. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, does not properly validate the whole certificate chain. **CVE ID : CVE-2019-18826**	N/A	O-BAR-CLIC-060120/1104
Improper Input Validation	16-12-2019	4.3	On Barco ClickShare Button R9861500D01 devices (before firmware version 1.9.0) JTAG access is disabled after ROM code execution. This means that JTAG access is possible when the system is running code from ROM before handing control over to embedded firmware. **CVE ID : CVE-2019-18827**	N/A	O-BAR-CLIC-060120/1105
Insufficiently Protected Credentials	16-12-2019	7.2	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Insufficiently Protected Credentials. The root	N/A	O-BAR-CLIC-060120/1106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			account (present for access via debug interfaces, which are by default not enabled on production devices) of the embedded Linux on the ClickShare Button is using a weak password. **CVE ID : CVE-2019-18828**		
clickshare_cse-800_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-12-2019	10	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow OS Command Injection. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, is vulnerable to OS command injection vulnerabilities. These vulnerabilities could lead to code execution on the ClickShare Button with the privileges of the user 'nobody'. **CVE ID : CVE-2019-18830**	N/A	O-BAR-CLIC-060120/1107
Information Exposure	16-12-2019	3.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information Exposure. The encrypted ClickShare Button firmware contains the private key of a test device-certificate. **CVE ID : CVE-2019-18831**	N/A	O-BAR-CLIC-060120/1108
Improper Certificate Validation	16-12-2019	7.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Improper Following of a Certificate's	N/A	O-BAR-CLIC-060120/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Chain of Trust. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, does not properly validate the whole certificate chain. **CVE ID : CVE-2019-18826**		
Improper Input Validation	16-12-2019	4.3	On Barco ClickShare Button R9861500D01 devices (before firmware version 1.9.0) JTAG access is disabled after ROM code execution. This means that JTAG access is possible when the system is running code from ROM before handing control over to embedded firmware. **CVE ID : CVE-2019-18827**	N/A	O-BAR-CLIC-060120/1110
Insufficiently Protected Credentials	16-12-2019	7.2	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Insufficiently Protected Credentials. The root account (present for access via debug interfaces, which are by default not enabled on production devices) of the embedded Linux on the ClickShare Button is using a weak password. **CVE ID : CVE-2019-18828**	N/A	O-BAR-CLIC-060120/1111
Canonical					
ubuntu_linux					
Weak Password Recovery	18-12-2019	5	Django before 1.11.27, 2.x before 2.2.9, and 3.x before 3.0.1 allows account	https://www.djangoproject.com/	O-CAN-UBUN-060120/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Mechanism for Forgotten Password			takeover. A suitably crafted email address (that is equal to an existing user's email address after case transformation of Unicode characters) would allow an attacker to be sent a password reset token for the matched user account. (One mitigation in the new releases is to send password reset tokens only to the registered user email address.) **CVE ID : CVE-2019-19844**	weblog/2019/dec/18/security-releases/	
Debian					
debian_linux					
Improper Resource Shutdown or Release	16-12-2019	5	knot-resolver before version 4.3.0 is vulnerable to denial of service through high CPU utilization. DNS replies with very many resource records might be processed very inefficiently, in extreme cases taking even several CPU seconds for each such uncached message. For example, a few thousand A records can be squashed into one DNS message (limit is 64kB). **CVE ID : CVE-2019-19331**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-19331	O-DEB-DEBI-060120/1113
Improper Input Validation	16-12-2019	3.5	An issue was discovered in Cyrus IMAP before 2.5.15, 3.0.x before 3.0.13, and 3.1.x through 3.1.8. If sieve script uploading is allowed (3.x) or certain non-default sieve options are enabled (2.x), a	N/A	O-DEB-DEBI-060120/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user with a mail account on the service can use a sieve script containing a fileinto directive to create any mailbox with administrator privileges, because of folder mishandling in autosieve_createfolder() in imap/lmtp_sieve.c. **CVE ID : CVE-2019-19783**		
Improper Input Validation	17-12-2019	4	_core_/plugins/medias in SPIP 3.2.x before 3.2.7 allows remote authenticated authors to inject content into the database. **CVE ID : CVE-2019-19830**	N/A	O-DEB-DEBI-060120/1115
Dell					
xps_7390_firmware					
N/A	16-12-2019	7.2	Settings for the Dell XPS 13 2-in-1 (7390) BIOS versions prior to 1.1.3 contain a configuration vulnerability. The BIOS configuration for the "Enable Thunderbolt (and PCIe behind TBT) pre-boot modules" setting is enabled by default. A local unauthenticated attacker with physical access to a user's system can obtain read or write access to main memory via a DMA attack during platform boot. **CVE ID : CVE-2019-18579**	N/A	O-DEL-XPS_-060120/1116
Dlink					
dir-615_t1_firmware					
Improper Input	16-12-2019	4	On D-Link DIR-615 devices, a normal user is able to	N/A	O-DLI-DIR--060120/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			create a root(admin) user from the D-Link portal. **CVE ID : CVE-2019-19743**		
dir-615_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	3.5	On D-Link DIR-615 devices, the User Account Configuration page is vulnerable to blind XSS via the name field. **CVE ID : CVE-2019-19742**	N/A	O-DLI-DIR--060120/1118
Google					
android					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-12-2019	6.8	An injection issue was addressed with improved validation. This issue is fixed in Shazam Android App Version 9.25.0, Shazam iOS App Version 12.11.0. Processing a maliciously crafted URL may lead to arbitrary javascript code execution. **CVE ID : CVE-2019-8792**	N/A	O-GOO-ANDR-060120/1119
Weak Password Requirements	18-12-2019	7.5	Trend Micro Mobile Security for Android (Consumer) versions 10.3.1 and below on Android 8.0+ has an issue in which an attacker could bypass the product's App Password Protection feature. **CVE ID : CVE-2019-19690**	N/A	O-GOO-ANDR-060120/1120
Huawei					
elle-al00b_firmware					
Buffer Copy without	23-12-2019	5.8	Huawei smart phones with earlier versions than ELLE-	https://www.huawei.c	O-HUA-ELLE-060120/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			AL00B 9.1.0.222(C00E220R2P1) have a buffer overflow vulnerability. An attacker may intercept and tamper with the packet in the local area network (LAN) to exploit this vulnerability. Successful exploitation may cause the affected phone abnormal. **CVE ID : CVE-2019-5276**	om/en/psirt/security-advisories/huawei-sa-20191218-02-smartphone-en	
oceanstor_sns3096_firmware					
Information Exposure	23-12-2019	2.1	Huawei OceanStor SNS3096 V100R002C01 have an information disclosure vulnerability. Attackers with low privilege can exploit this vulnerability by performing some specific operations. Successful exploit of this vulnerability can cause some information disclosure. **CVE ID : CVE-2019-5267**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191218-03-information-en	O-HUA-OCEA-060120/1122
p30_firmware					
Information Exposure	23-12-2019	5	Huawei Share function in P30 9.1.0.193(C00E190R2P1) smartphone has an improper access control vulnerability. The function incorrectly controls certain access messages, attackers can simulate a sender to steal P2P network information. Successful exploit may cause information leakage. **CVE ID : CVE-2019-5265**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191218-01-share-en	O-HUA-P30_-060120/1123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-12-2019	5	Huawei Share function in P30 9.1.0.193(C00E190R2P1) smartphone has an insufficient input validation vulnerability. Attackers can exploit this vulnerability by sending crafted packets to the affected device. Successful exploit may cause the function will be disabled. **CVE ID : CVE-2019-5266**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191218-02-share-en	O-HUA-P30_-060120/1124
humaxdigital					
hgb10r-2_firmware					
Cleartext Transmission of Sensitive Information	18-12-2019	5	An issue was discovered on Humax Wireless Voice Gateway HGB10R-2 20160817_1855 devices. The attacker can discover admin credentials in the backup file, aka backupsettings.conf. **CVE ID : CVE-2019-19889**	N/A	O-HUM-HGB1-060120/1125
Insufficiently Protected Credentials	18-12-2019	5	An issue was discovered on Humax Wireless Voice Gateway HGB10R-2 20160817_1855 devices. Admin credentials are sent over cleartext HTTP. **CVE ID : CVE-2019-19890**	N/A	O-HUM-HGB1-060120/1126
Linux					
linux_kernel					
Improper Privilege Management	17-12-2019	4.6	In the Linux kernel before 5.4.2, the io_uring feature leads to requests that inadvertently have UID 0 and full capabilities, aka CID-181e448d8709. This is	N/A	O-LIN-LINU-060120/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			related to fs/io-wq.c, fs/io_uring.c, and net/socket.c. For example, an attacker can bypass intended restrictions on adding an IPv4 address to the loopback interface. This occurs because IORING_OP_SENDMSG operations, although requested in the context of an unprivileged user, are sometimes performed by a kernel worker thread without considering that context. **CVE ID : CVE-2019-19241**		
Use After Free	17-12-2019	9.3	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image, performing some operations, and then making a syncfs system call can lead to a use-after-free in __mutex_lock in kernel/locking/mutex.c. This is related to mutex_can_spin_on_owner in kernel/locking/mutex.c, __btrfs_qgroup_free_meta in fs/btrfs/qgroup.c, and btrfs_insert_delayed_items in fs/btrfs/delayed-inode.c. **CVE ID : CVE-2019-19813**	N/A	O-LIN-LINU-060120/1128
Out-of-bounds Write	17-12-2019	9.3	In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause __remove_dirty_segment slab-out-of-bounds write access because an array is bounded by the number of	N/A	O-LIN-LINU-060120/1129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			dirty types (8) but the array index can exceed this. **CVE ID : CVE-2019-19814**		
NULL Pointer Dereference	17-12-2019	7.1	In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause a NULL pointer dereference in f2fs_recover_fsync_data in fs/f2fs/recovery.c. This is related to F2FS_P_SB in fs/f2fs/f2fs.h. **CVE ID : CVE-2019-19815**	N/A	O-LIN-LINU-060120/1130
Out-of-bounds Write	17-12-2019	9.3	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image and performing some operations can cause slab-out-of-bounds write access in __btrfs_map_block in fs/btrfs/volumes.c, because a value of 1 for the number of data stripes is mishandled. **CVE ID : CVE-2019-19816**	N/A	O-LIN-LINU-060120/1131
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-12-2019	10	Brackets versions 1.14 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8255**	https://helpx.adobe.com/security/products/brackets/apsb19-57.html	O-LIN-LINU-060120/1132
Microsoft					
windows					
Improper Privilege Management	19-12-2019	7.5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155	https://helpx.adobe.com/security/products/	O-MIC-WIND-060120/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a binary planting (default folder privilege escalation) vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2019-16444**	acrobat/apsb19-55.html	
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16445**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1134
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16446**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1135
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155	https://helpx.adobe.com/security/products/	O-MIC-WIND-060120/1136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16448**	acrobat/apsb19-55.html	
Information Exposure	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16449**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1137
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16450**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1138
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version,	https://helpx.adobe.com/security/products/acrobat/aps	O-MIC-WIND-060120/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2017.011.30152 and earlier, and 2015.006.30505 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16451**	b19-55.html	
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16452**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1140
Improper Input Validation	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a security bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-16453**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1141
Out-of-bounds Write	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16454**		
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16455**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1143
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16456**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1144
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16457**		
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16458**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1146
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16459**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1147
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16460**		
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16461**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1149
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16462**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1150
NULL Pointer Dereference	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16463**		
Use After Free	19-12-2019	10	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2019-16464**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1152
Out-of-bounds Read	19-12-2019	5	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2019-16465**	https://helpx.adobe.com/security/products/acrobat/apsb19-55.html	O-MIC-WIND-060120/1153
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-12-2019	9.3	Adobe Photoshop CC versions before 20.0.8 and 21.0.x before 21.0.2 have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8253**	https://helpx.adobe.com/security/products/photoshop/apsb19-56.html	O-MIC-WIND-060120/1154
Improper Restriction	19-12-2019	9.3	Adobe Photoshop CC versions before 20.0.8 and	https://helpx.adobe.co	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			21.0.x before 21.0.2 have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8254**	m/security/products/photoshop/apsb19-56.html	060120/1155
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-12-2019	10	Brackets versions 1.14 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-8255**	https://helpx.adobe.com/security/products/brackets/apsb19-57.html	O-MIC-WIND-060120/1156
windows_10					
Information Exposure	16-12-2019	2.1	Insufficient memory protection for Intel(R) Ethernet I218 Adapter driver for Windows* 10 before version 24.1 may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-11096**	N/A	O-MIC-WIND-060120/1157
Improper Input Validation	18-12-2019	6.9	AsLdrSrv.exe in ASUS ATK Package before V1.0.0061 (for Windows 10 notebook PCs) could lead to unsigned code execution with no additional execution. The user must put an application at a particular path, with a particular file name. **CVE ID : CVE-2019-19235**	https://www.asus.com/Static_WebPage/ASUS-Product-Security-Advisory/	O-MIC-WIND-060120/1158
Omron					
plc_cj_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	16-12-2019	7.5	In Omron PLC CJ series, all versions and Omron PLC CS series, all versions, an attacker could spoof arbitrary messages or execute commands. **CVE ID : CVE-2019-18259**	N/A	O-OMR-PLC_-060120/1159
Improper Restriction of Excessive Authentication Attempts	16-12-2019	5	In Omron PLC CS series, all versions, Omron PLC CJ series, all versions, and Omron PLC NJ series, all versions, the software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks. **CVE ID : CVE-2019-18261**	N/A	O-OMR-PLC_-060120/1160
N/A	16-12-2019	7.5	In Omron PLC CJ series, all versions, and Omron PLC CS series, all versions, the software properly checks for the existence of a lock, but the lock can be externally controlled or influenced by an actor that is outside of the intended sphere of control. **CVE ID : CVE-2019-18269**	N/A	O-OMR-PLC_-060120/1161
plc_cs_firmware					
Authentication Bypass by Spoofing	16-12-2019	7.5	In Omron PLC CJ series, all versions and Omron PLC CS series, all versions, an attacker could spoof arbitrary messages or execute commands. **CVE ID : CVE-2019-18259**	N/A	O-OMR-PLC_-060120/1162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	16-12-2019	5	In Omron PLC CS series, all versions, Omron PLC CJ series, all versions, and Omron PLC NJ series, all versions, the software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks. **CVE ID : CVE-2019-18261**	N/A	O-OMR-PLC_-060120/1163
N/A	16-12-2019	7.5	In Omron PLC CJ series, all versions, and Omron PLC CS series, all versions, the software properly checks for the existence of a lock, but the lock can be externally controlled or influenced by an actor that is outside of the intended sphere of control. **CVE ID : CVE-2019-18269**	N/A	O-OMR-PLC_-060120/1164
plc_nj_firmware					
Improper Restriction of Excessive Authentication Attempts	16-12-2019	5	In Omron PLC CS series, all versions, Omron PLC CJ series, all versions, and Omron PLC NJ series, all versions, the software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks. **CVE ID : CVE-2019-18261**	N/A	O-OMR-PLC_-060120/1165
Qualcomm					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6574au_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1166
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which	https://www.qualcomm.com/company/produ	O-QUA-QCA6-060120/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	ct-security/bulletins/december-2019-bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1170
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1173
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10601		
qcs405_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1176
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1178

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1181
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10564		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1184
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-QCS4-060120/1185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150 **CVE ID : CVE-2019-10601**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS4-060120/1188
ipq4019_firmware					
Buffer Copy without	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of	https://www.qualcom	O-QUA-IPQ4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	m.com/company/product-security/bulletins/december-2019-bulletin	060120/1189
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ4-060120/1190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ4-060120/1191
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon	https://www.qualcomm.com/company/produ	O-QUA-IPQ4-060120/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	ct-security/bulletins/december-2019-bulletin	
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ4-060120/1193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ4-060120/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ4-060120/1195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ4-060120/1196
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-IPQ4-060120/1197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	mber-2019-bulletin	
ipq8064_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1200
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1205
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
ipq8074_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1209
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1214
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-IPQ8-060120/1217
qca6174a_firmware					
Buffer Copy without Checking Size of Input	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received	https://www.qualcomm.com/company/produ	O-QUA-QCA6-060120/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	ct-security/bulletins/december-2019-bulletin	
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA6-060120/1221
qca9377_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA9-060120/1222
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to	https://www.qualcomm.com/company/product-security/bu	O-QUA-QCA9-060120/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-QCA9-060120/1224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	bulletin	
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA9-060120/1225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
qca9379_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA9-060120/1226
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives	https://www.qualcom	O-QUA-QCA9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	m.com/company/product-security/bulletins/december-2019-bulletin	060120/1227
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-	O-QUA-QCA9-060120/1228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	security/bulletins/december-2019-bulletin	
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA9-060120/1229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
apq8009_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1231
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in	https://www.qualcomm.com/com	O-QUA-APQ8-060120/1232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-APQ8-060120/1233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	mber-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1236

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1238
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as	https://www.qualcomm.com/company/product-	O-QUA-APQ8-060120/1239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-APQ8-060120/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	bulletin	
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1242
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-APQ8-060120/1243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1247
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
apq8098_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1252
Information	18-12-2019	7.1	Due to the use of non-time-	https://ww	O-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/1253
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in	https://www.qualcomm.com/company/product-	O-QUA-APQ8-060120/1254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1259
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives	https://www.qualcom	O-QUA-APQ8-060120/1260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	m.com/company/product-security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in	https://www.qualcomm.com/company/product-	O-QUA-APQ8-060120/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1264

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1266
Integer	18-12-2019	10	Device memory may get	https://ww	O-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/1267
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-APQ8-060120/1268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	bulletin	
msm8939_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1273
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1278
Buffer Copy without Checking	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range	https://www.qualcomm.com/com	O-QUA-MSM8-060120/1279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	pany/product-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
msm8953_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10482		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1284
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in	https://www.qualcomm.com/com	O-QUA-MSM8-060120/1285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MSM8-060120/1286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	lletins/december-2019-bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1291
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MSM8-060120/1292

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 Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2242		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1297
msm8998_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MSM8-060120/1298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	bulletin	
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1302

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1304
Double Free	18-12-2019	7.2	Potential double free	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MSM8-060120/1305
Improper Restriction of Operations	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access	https://www.qualcomm.com/company/produ	O-QUA-MSM8-060120/1306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	ct-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1311
Improper Authenticati on	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in	https://www.qualcomm.com/com	O-QUA-MSM8-060120/1312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	pany/product-security/bulletins/december-2019-bulletin	
nicobar_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1315

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10525		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1319
Integer	18-12-2019	7.2	Improper validation of event	https://ww	O-QUA-NICO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/1320
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1322
Out-of-	18-12-2019	4.6	Possibility of out of bound	https://ww	O-QUA-NICO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/1323
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-NICO-060120/1327
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-NICO-060120/1328

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	mber-2019-bulletin	
apq8053_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1334
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in	https://www.qualcomm.com/com	O-QUA-APQ8-060120/1335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	pany/product-security/bulletins/december-2019-bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1340
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1343
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-APQ8-060120/1344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	lletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1347
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1351
mdm9207c_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1352
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MDM9-060120/1353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	lletins/december-2019-bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MDM9-060120/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1358
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1361
NULL	18-12-2019	7.2	Use of local variable as	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MDM9-060120/1362
Buffer Copy without Checking Size of Input ('Classic Buffer	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-MDM9-060120/1363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	mber-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
msm8905_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1366

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1369

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1370
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list	https://www.qualcomm.com/com	O-QUA-MSM8-060120/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	pany/product-security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MSM8-060120/1372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
qcn7605_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCN7-060120/1376
Buffer Copy without Checking Size of Input ('Classic Buffer	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-QCN7-060120/1377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	mber-2019-bulletin	
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCN7-060120/1378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCN7-060120/1379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCN7-060120/1380
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCN7-060120/1381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCN7-060120/1382

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCN7-060120/1383
Buffer Copy without Checking Size of Input ('Classic Buffer	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not	https://www.qualcomm.com/company/product-security/bu	O-QUA-QCN7-060120/1384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	lletins/december-2019-bulletin	
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCN7-060120/1385
Buffer Copy without	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling	https://www.qualcom	O-QUA-QCN7-060120/1386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	m.com/company/product-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCN7-060120/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCN7-060120/1388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Improper Authenticati on	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCN7-060120/1389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdm845_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1390
Buffer Copy without Checking Size of Input	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from	https://www.qualcomm.com/company/produ	O-QUA-SDM8-060120/1391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	ct-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1396
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in	https://www.qualcomm.com/com	O-QUA-SDM8-060120/1397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	pany/product-security/bulletins/december-2019-bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1401
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1405
Buffer Copy without Checking Size of Input ('Classic	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that	https://www.qualcomm.com/company/product-	O-QUA-SDM8-060120/1406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1408
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-SDM8-060120/1409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	mber-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1411

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
apq8017_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1412

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-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10480		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1414
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA	https://www.qualcom	O-QUA-APQ8-060120/1415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	m.com/company/product-security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-APQ8-060120/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	mber-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1418

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1421
Improper Restriction of	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can	https://www.qualcomm.com/com	O-QUA-APQ8-060120/1422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-APQ8-060120/1423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1425
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope	https://www.qualcomm.com/com	O-QUA-APQ8-060120/1426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	pany/product-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-APQ8-060120/1427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
apq8096au_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1432
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon	https://www.qualcomm.com/company/product-security/bu	O-QUA-APQ8-060120/1433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	lletins/december-2019-bulletin	
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1435

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1437
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent	https://www.qualcom	O-QUA-APQ8-060120/1438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	m.com/company/product-security/bulletins/december-2019-bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1443
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10595		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1447
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1450
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of	https://www.qualcomm.com/company/produ	O-QUA-APQ8-060120/1451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	ct-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
sda845_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1455
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in	https://www.qualcomm.com/com	O-QUA-SDA8-060120/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-SDA8-060120/1457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	mber-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1462
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as	https://www.qualcomm.com/company/product-	O-QUA-SDA8-060120/1463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDA8-060120/1464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	bulletin	
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1466
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDA8-060120/1467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1470
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDA8-060120/1471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	lletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA8-060120/1473

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sdm636_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1474

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-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1476
Out-of-	18-12-2019	10	Buffer over read can happen	https://ww	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/1477
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM6-060120/1478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDM6-060120/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10525		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1483
Improper	18-12-2019	4.6	Improper length check on	https://ww	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/1484
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-SDM6-060120/1485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	mber-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1487
Improper	18-12-2019	7.2	Possible buffer overwrite in	https://ww	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/1488
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1491
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1494
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in	https://www.qualcomm.com/com	O-QUA-SDM6-060120/1495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	pany/product-security/bulletins/december-2019-bulletin	
sdm670_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1497

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1499

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1501

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1502
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM6-060120/1503

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	lletins/december-2019-bulletin	
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1507
Out-of-	18-12-2019	4.6	Possibility of out of bound	https://ww	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/1508
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authenticati on	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2274**		
sdm710_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1513
Buffer Copy without	18-12-2019	7.2	Out of bound write can happen in WMI firmware	https://www.qualcom	O-QUA-SDM7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	m.com/company/product-security/bulletins/december-2019-bulletin	060120/1514
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDM7-060120/1515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1518

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1522
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory	https://www.qualcomm.com/com	O-QUA-SDM7-060120/1523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	pany/product-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10600		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1527
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto,	https://www.qualcomm.com/company/produ	O-QUA-SDM7-060120/1528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	ct-security/bulletins/december-2019-bulletin	
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM7-060120/1529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sm6150_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1531
Buffer Copy without	18-12-2019	7.2	Out of bound write can happen in WMI firmware	https://www.qualcom	O-QUA-SM61-060120/1532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	m.com/company/product-security/bulletins/december-2019-bulletin	
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SM61-060120/1533

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 APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	bulletin	
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1537
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in	https://www.qualcomm.com/com	O-QUA-SM61-060120/1538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	pany/product-security/bulletins/december-2019-bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1542
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1546
Buffer Copy without Checking Size of Input ('Classic	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that	https://www.qualcomm.com/company/product-	O-QUA-SM61-060120/1547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1549
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-SM61-060120/1550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	mber-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM61-060120/1552

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
qm215_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QM21-060120/1553

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-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QM21-060120/1554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QM21-060120/1555
NULL Pointer	18-12-2019	4.9	Possibility of Null pointer access if the SPDM	https://www.qualcom	O-QUA-QM21-060120/1556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	m.com/company/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QM21-060120/1557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QM21-060120/1558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QM21-060120/1559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QM21-060120/1560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QM21-060120/1561
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted	https://www.qualcomm.com/com	O-QUA-QM21-060120/1562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	pany/product-security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QM21-060120/1563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QM21-060120/1564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QM21-060120/1565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authenticati on	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QM21-060120/1566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca8081_firmware					
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA8-060120/1567
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA8-060120/1568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA8-060120/1569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA8-060120/1570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA8-060120/1571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA8-060120/1572
qcs404_firmware					
Information	18-12-2019	7.1	Due to the use of non-time-constant comparison	https://www.qualcom	O-QUA-QCS4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	m.com/company/product-security/bulletins/december-2019-bulletin	060120/1573
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-QCS4-060120/1574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	lletins/december-2019-bulletin	
sm8150_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-SM81-060120/1575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	mber-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1578
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1581

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1583
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SM81-060120/1584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	lletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2019-10537**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1588
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory	https://www.qualcomm.com/com	O-QUA-SM81-060120/1589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	pany/product-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1592
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10607		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM81-060120/1596
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto,	https://www.qualcomm.com/company/produ	O-QUA-SM81-060120/1597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	ct-security/bulletins/december-2019-bulletin	
mdm9206_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1601

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1603
Double Free	18-12-2019	4.6	Memory is being freed up	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MDM9-060120/1604
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1609
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1613
Buffer Copy without Checking	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character	https://www.qualcomm.com/com	O-QUA-MDM9-060120/1614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-MDM9-060120/1615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	mber-2019-bulletin	
mdm9607_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10480		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1619
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1624
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1627

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1629
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MDM9-060120/1630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	lletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1633
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1636
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
mdm9650_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1643
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-MDM9-060120/1644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MDM9-060120/1645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1650
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MDM9-060120/1651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	lletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1654
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1658
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in	https://www.qualcomm.com/com	O-QUA-MDM9-060120/1659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	pany/product-security/bulletins/december-2019-bulletin	
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
mdm9655_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10525		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1665
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-MDM9-060120/1666

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 APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	security/bulletins/december-2019-bulletin	
msm8996au_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1669
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which	https://www.qualcomm.com/company/produ	O-QUA-MSM8-060120/1670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	ct-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MSM8-060120/1671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1675
Out-of-	18-12-2019	10	Buffer overflow during SIB	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MSM8-060120/1676
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to	https://www.qualcomm.com/company/product-security/bu	O-QUA-MSM8-060120/1677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	lletins/december-2019-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MSM8-060120/1678

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	bulletin	
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1681
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MSM8-060120/1682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1684
Improper	18-12-2019	7.2	Out of bound access can	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MSM8-060120/1685
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
mdm9615_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1690
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in	https://www.qualcomm.com/company/product-	O-QUA-MDM9-060120/1691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	security/bulletins/december-2019-bulletin	
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
mdm9625_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1695

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-2019-10500**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1697
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list	https://www.qualcomm.com/com	O-QUA-MDM9-060120/1698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	pany/product-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MDM9-060120/1699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	bulletin	
mdm9205_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
msm8909_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1706
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI	https://www.qualcomm.com/company/product-security/bu	O-QUA-MSM8-060120/1707

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1710

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1711

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1712
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list	https://www.qualcomm.com/com	O-QUA-MSM8-060120/1713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	pany/product-security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MSM8-060120/1714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	bulletin	
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1717
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-MSM8-060120/1718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	mber-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
mdm9635m_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1721

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1722

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1723

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/1724
qca9531_firmware					
Buffer Copy without	18-12-2019	7.2	Out of bounds memcpy can occur by providing the	https://www.qualcom	O-QUA-QCA9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	m.com/company/product-security/bulletins/december-2019-bulletin	060120/1725
qca9880_firmware					
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets	https://www.qualcomm.com/company/produ	O-QUA-QCA9-060120/1726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	ct-security/bulletins/december-2019-bulletin	
qca9886_firmware					
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA9-060120/1727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA9-060120/1728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
qca9980_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA9-060120/1729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA9-060120/1730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA9-060120/1731
sdm429_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1732
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM4-060120/1733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1736

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1738

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-2019-10525**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10544		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1740
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1745
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-SDM4-060120/1746

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 APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	mber-2019-bulletin	
sdm632_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1749

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1752
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list	https://www.qualcomm.com/com	O-QUA-SDM6-060120/1753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	pany/product-security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDM6-060120/1754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1757
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead	https://www.qualcomm.com/company/produ	O-QUA-SDM6-060120/1758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	ct-security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
msm8917_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1763
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1767

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1769
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1774
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in	https://www.qualcomm.com/company/product-	O-QUA-MSM8-060120/1775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1780
Improper Authenticati	18-12-2019	7.2	Improper Access Control for RPU write access from	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	m.com/company/product-security/bulletins/december-2019-bulletin	060120/1781
msm8920_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10480		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1785
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	m.com/company/product-security/bulletins/december-2019-bulletin	060120/1786
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-MSM8-060120/1787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	mber-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1792
Improper Restriction of	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can	https://www.qualcomm.com/com	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	pany/product-security/bulletins/december-2019-bulletin	060120/1793
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MSM8-060120/1794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10614		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1799
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-MSM8-060120/1800

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 APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	security/bulletins/december-2019-bulletin	
msm8937_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1803
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	m.com/company/product-security/bulletins/december-2019-bulletin	060120/1804
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MSM8-060120/1805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	lletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10518		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1810
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another	https://www.qualcomm.com/com	O-QUA-MSM8-060120/1811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	pany/product-security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the Bounds of a	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MSM8-060120/1812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	lletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1817
Integer Overflow or	18-12-2019	10	Device memory may get corrupted because of buffer	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	m.com/company/product-security/bulletins/december-2019-bulletin	060120/1818
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MSM8-060120/1819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	bulletin	
msm8940_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1822
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI	https://www.qualcomm.com/company/product-security/bu	O-QUA-MSM8-060120/1823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1825

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1826

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1827

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1828
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list	https://www.qualcomm.com/com	O-QUA-MSM8-060120/1829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	pany/product-security/bulletins/december-2019-bulletin	
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MSM8-060120/1830

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1831

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1835
Out-of-	18-12-2019	7.5	Out of boundary access is	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MSM8-060120/1836
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-MSM8-060120/1837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	mber-2019-bulletin	
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
msm8996_firmware					
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1840

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/1841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
sdm450_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1844
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SDM4-060120/1845

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDM4-060120/1846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1850
Integer Overflow or	18-12-2019	7.5	Improper check in video driver while processing data	https://www.qualcom	O-QUA-SDM4-060120/1851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	m.com/company/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDM4-060120/1852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1855

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1856
sm8250_firmware					
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential	https://www.qualcomm.com/company/product-	O-QUA-SM82-060120/1857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	security/bulletins/december-2019-bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SM82-060120/1858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM82-060120/1859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM82-060120/1860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM82-060120/1861
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM82-060120/1862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM82-060120/1863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM82-060120/1864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10584		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM82-060120/1865
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of	https://www.qualcomm.com/company/produ	O-QUA-SM82-060120/1866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	ct-security/bulletins/december-2019-bulletin	
sxr2130_firmware					
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SXR2-060120/1867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR2-060120/1868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR2-060120/1869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR2-060120/1870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR2-060120/1871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR2-060120/1872
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR2-060120/1873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR2-060120/1874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR2-060120/1875
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in	https://www.qualcomm.com/company/product-	O-QUA-SXR2-060120/1876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR2-060120/1877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
apq8016_firmware					
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
sa6155p_firmware					
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SA61-060120/1879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SA61-060120/1880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SA61-060120/1881
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto,	https://www.qualcomm.com/company/produ	O-QUA-SA61-060120/1882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	ct-security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SA61-060120/1883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SA61-060120/1884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
sc8180x_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SC81-060120/1885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SC81-060120/1886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SC81-060120/1887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SC81-060120/1888
Out-of-bounds	18-12-2019	10	Buffer overflow during SIB read when network	https://www.qualcom	O-QUA-SC81-060120/1889

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	m.com/company/product-security/bulletins/december-2019-bulletin	
sdm850_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SDM8-060120/1890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	security/bulletins/december-2019-bulletin	
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1895

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10525**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2242		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM8-060120/1897
qcm2150_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-QCM2-060120/1898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCM2-060120/1899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCM2-060120/1900

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCM2-060120/1901

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCM2-060120/1902

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
sdx55_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1904
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1907
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SDX5-060120/1908

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDX5-060120/1909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1913
Improper Restriction of Operations within the	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in	https://www.qualcomm.com/company/product-	O-QUA-SDX5-060120/1914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1916
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in	https://www.qualcomm.com/company/product-	O-QUA-SDX5-060120/1917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1920
Buffer Copy without Checking	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character	https://www.qualcomm.com/com	O-QUA-SDX5-060120/1921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-SDX5-060120/1922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	mber-2019-bulletin	
Improper Authenticati on	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX5-060120/1923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
apq8064_firmware					
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
apq8096_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1927
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which	https://www.qualcomm.com/company/produ	O-QUA-APQ8-060120/1928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	ct-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-APQ8-060120/1929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-APQ8-060120/1934
sda660_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SDA6-060120/1935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1939

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1940

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-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1941
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDA6-060120/1942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1946
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDA6-060120/1947

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 Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1950
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDA6-060120/1951

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 APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1952

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDA6-060120/1954
Improper Authenticati	18-12-2019	7.2	Improper Access Control for RPU write access from	https://www.qualcom	O-QUA-SDA6-060120/1955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	m.com/company/product-security/bulletins/december-2019-bulletin	
sdm439_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1959

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1960

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-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10518		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1962
Improper Restriction of	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can	https://www.qualcomm.com/com	O-QUA-SDM4-060120/1963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDM4-060120/1964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10584		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1967
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of	https://www.qualcomm.com/company/produ	O-QUA-SDM4-060120/1968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	ct-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM4-060120/1969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authenticati on	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655,	https://ww w.qualcom m.com/com pany/produ ct-security/bu lletins/dece mber-2019-bulletin	O-QUA-SDM4-060120/1970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sdm630_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1974
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SDM6-060120/1975

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDM6-060120/1976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1981
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM6-060120/1982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	lletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1985
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1988
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1991
Improper Authenticati	18-12-2019	7.2	Improper Access Control for RPU write access from	https://www.qualcom	O-QUA-SDM6-060120/1992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	m.com/company/product-security/bulletins/december-2019-bulletin	
sdm660_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10480		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1996
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA	https://www.qualcom	O-QUA-SDM6-060120/1997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	m.com/company/product-security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-SDM6-060120/1998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	mber-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/1999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2003
Integer Overflow or	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer	https://www.qualcomm.com/com	O-QUA-SDM6-060120/2004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	pany/product-security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2006
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM6-060120/2007

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 Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2010
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDM6-060120/2011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	bulletin	
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2013
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDM6-060120/2016

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
mdm9150_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2017

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2018
Out-of-	18-12-2019	10	Buffer over read can happen	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MDM9-060120/2019
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MDM9-060120/2020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-MDM9-060120/2021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2023

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2024

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2026
mdm9640_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-MDM9-060120/2027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	mber-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2029

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2030

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10525		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2033
Improper	18-12-2019	4.6	Improper length check on	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MDM9-060120/2034
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-MDM9-060120/2035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	mber-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2038

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2039
Integer	18-12-2019	10	Device memory may get	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MDM9-060120/2040
msm8909w_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MSM8-060120/2041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	lletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2045

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2046
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-MSM8-060120/2047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2051
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted	https://www.qualcomm.com/com	O-QUA-MSM8-060120/2052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	pany/product-security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MSM8-060120/2056

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
qcs605_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2058
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2060

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2061

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2064
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2068
Improper Restriction of	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can	https://www.qualcomm.com/com	O-QUA-QCS6-060120/2069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-QCS6-060120/2070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2071
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can	https://www.qualcomm.com/com	O-QUA-QCS6-060120/2072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2075
Buffer Copy	18-12-2019	7.2	Out of bounds memcpy can	https://ww	O-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/2076
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of	https://www.qualcomm.com/company/product-	O-QUA-QCS6-060120/2077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCS6-060120/2079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sdx20_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2082
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service	https://www.qualcom	O-QUA-SDX2-060120/2083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	m.com/company/product-security/bulletins/december-2019-bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDX2-060120/2084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2086

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-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2088
Out-of-	18-12-2019	10	Out-of-bound read in the	https://ww	O-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/2089
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2092
Buffer Copy without Checking Size of Input ('Classic	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that	https://www.qualcomm.com/company/product-	O-QUA-SDX2-060120/2093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2095
Buffer Copy without Checking Size of Input ('Classic Buffer	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDX2-060120/2096

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 IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	lletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sm7150_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2101
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150 **CVE ID : CVE-2019-10481**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2104
Out-of-	18-12-2019	10	Buffer over read can happen	https://ww	O-QUA-SM71-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/2105
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SM71-060120/2106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SM71-060120/2107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10525		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2111
Integer	18-12-2019	7.2	Improper validation of event	https://ww	O-QUA-SM71-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/2112
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2115
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-SM71-060120/2116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	mber-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2119
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SM71-060120/2122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2274		
sxr1130_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2123
Buffer Copy without Checking	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event	https://www.qualcomm.com/com	O-QUA-SXR1-060120/2124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	pany/product-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2129
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in	https://www.qualcomm.com/com	O-QUA-SXR1-060120/2130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	pany/product-security/bulletins/december-2019-bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2134
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2137
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2140
NULL	18-12-2019	7.2	Use of local variable as	https://ww	O-QUA-SXR1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/2141
Buffer Copy without Checking Size of Input ('Classic Buffer	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	O-QUA-SXR1-060120/2142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	mber-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SXR1-060120/2145

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sdx24_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2147
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2149

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2150

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2152

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2153
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list	https://www.qualcomm.com/com	O-QUA-SDX2-060120/2154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	pany/product-security/bulletins/december-2019-bulletin	
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-SDX2-060120/2155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2159
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDX2-060120/2160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	lletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2163
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-SDX2-060120/2165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
mdm9645_firmware					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2167

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10516		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-MDM9-060120/2169
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in	https://www.qualcomm.com/com	O-QUA-MDM9-060120/2170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	pany/product-security/bulletins/december-2019-bulletin	
qca4531_firmware					
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	O-QUA-QCA4-060120/2171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA4-060120/2172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
qca9558_firmware					
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA9-060120/2173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	O-QUA-QCA9-060120/2174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Sonicwall					
sma_100_firmware					
Information Exposure	17-12-2019	5	Vulnerability in SonicWall SMA100 allow unauthenticated user to gain read-only access to unauthorized resources. This vulnerablity impacted SMA100 version 9.0.0.3 and earlier. **CVE ID : CVE-2019-7481**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0016	O-SON-SMA_-060120/2175
Trendnet					
tew-651br_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-12-2019	10	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. OS command injection occurs through the get_set.ccp lanHostCfg_HostName_1.1.1.0.0 parameter. **CVE ID : CVE-2019-11399**	N/A	O-TRE-TEW--060120/2176
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. A buffer overflow occurs through the get_set.ccp ccp_act parameter.	N/A	O-TRE-TEW--060120/2177

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-11400		
tew-652brp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-12-2019	10	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. OS command injection occurs through the get_set.ccp lanHostCfg_HostName_1.1.1.0.0 parameter. **CVE ID : CVE-2019-11399**	N/A	O-TRE-TEW--060120/2178
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. A buffer overflow occurs through the get_set.ccp ccp_act parameter. **CVE ID : CVE-2019-11400**	N/A	O-TRE-TEW--060120/2179
tew-652bru_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-12-2019	10	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. OS command injection occurs through the get_set.ccp lanHostCfg_HostName_1.1.1.0.0 parameter. **CVE ID : CVE-2019-11399**	N/A	O-TRE-TEW--060120/2180
Improper Restriction of Operations within the Bounds of a	18-12-2019	7.5	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. A buffer overflow occurs through the	N/A	O-TRE-TEW--060120/2181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			get_set.ccp ccp_act parameter. **CVE ID : CVE-2019-11400**		
Wago					
pfc_200_firmware					
Information Exposure	18-12-2019	5	An exploitable information exposure vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause an external tool to fail, resulting in uninitialized stack data to be copied to the response packet buffer. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5073**	N/A	O-WAG-PFC_-060120/2182
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	10	An exploitable stack buffer overflow vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware version 03.01.07(13), WAGO PFC200 Firmware version 03.00.39(12) and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a stack buffer overflow, resulting in code execution. An attacker can send unauthenticated packets to trigger this	https://talosintelligence.com/vulnerability_reports/TALOS-2019-0863	O-WAG-PFC_-060120/2183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. **CVE ID : CVE-2019-5074**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	10	An exploitable stack buffer overflow vulnerability exists in the command line utility getcouplerdetails of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets sent to the iocheckd service "I/O-Check" can cause a stack buffer overflow in the sub-process getcouplerdetails, resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5075**	N/A	O-WAG-PFC_-060120/2184
Missing Authenticati on for Critical Function	18-12-2019	8.5	An exploitable denial-of-service vulnerability exists in the iocheckd service ??I/O-Chec?? functionality of WAGO PFC 200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC 100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a denial of service, resulting in the device entering an error state where it ceases all network communications. An attacker can send unauthenticated packets to trigger this vulnerability.	N/A	O-WAG-PFC_-060120/2185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5077		
Missing Authenticati on for Critical Function	18-12-2019	9.4	An exploitable denial of service vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a denial of service, resulting in the device entering an error state where it ceases all network communications. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5078**	N/A	O-WAG-PFC_-060120/2186
Out-of-bounds Write	18-12-2019	7.5	An exploitable heap buffer overflow vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a heap buffer overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5079**	N/A	O-WAG-PFC_-060120/2187
Missing Authenticati on for	18-12-2019	6.4	An exploitable denial-of-service vulnerability exists in the iocheckd service "I/O-	N/A	O-WAG-PFC_-060120/2188

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Function			Check" functionality of WAGO PFC 200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A single packet can cause a denial of service and weaken credentials resulting in the default documented credentials being applied to the device. An attacker can send an unauthenticated packet to trigger this vulnerability. **CVE ID : CVE-2019-5080**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	10	An exploitable heap buffer overflow vulnerability exists in the iocheckd service ''I/O-Chec'' functionality of WAGO PFC 200 Firmware version 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a heap buffer overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5081**	N/A	O-WAG-PFC_-060120/2189
pfc_100_firmware					
Information Exposure	18-12-2019	5	An exploitable information exposure vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and	N/A	O-WAG-PFC_-060120/2190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause an external tool to fail, resulting in uninitialized stack data to be copied to the response packet buffer. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5073**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	10	An exploitable stack buffer overflow vulnerability exists in the iocheckd service ''I/O-Check'' functionality of WAGO PFC200 Firmware version 03.01.07(13), WAGO PFC200 Firmware version 03.00.39(12) and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a stack buffer overflow, resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5074**	https://talosintelligence.com/vulnerability_reports/TALOS-2019-0863	O-WAG-PFC_-060120/2191
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	10	An exploitable stack buffer overflow vulnerability exists in the command line utility getcouplerdetails of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets sent to	N/A	O-WAG-PFC_-060120/2192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the iocheckd service "I/O-Check" can cause a stack buffer overflow in the sub-process getcouplerdetails, resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5075**		
Missing Authenticati on for Critical Function	18-12-2019	8.5	An exploitable denial-of-service vulnerability exists in the iocheckd service ??I/O-Chec?? functionality of WAGO PFC 200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC 100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a denial of service, resulting in the device entering an error state where it ceases all network communications. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5077**	N/A	O-WAG-PFC_-060120/2193
Missing Authenticati on for Critical Function	18-12-2019	9.4	An exploitable denial of service vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a denial of service, resulting in the device	N/A	O-WAG-PFC_-060120/2194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			entering an error state where it ceases all network communications. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5078**		
Out-of-bounds Write	18-12-2019	7.5	An exploitable heap buffer overflow vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a heap buffer overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5079**	N/A	O-WAG-PFC_-060120/2195
Missing Authentication for Critical Function	18-12-2019	6.4	An exploitable denial-of-service vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC 200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A single packet can cause a denial of service and weaken credentials resulting in the default documented credentials being applied to the device. An attacker can send an unauthenticated	N/A	O-WAG-PFC_-060120/2196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packet to trigger this vulnerability. **CVE ID : CVE-2019-5080**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	10	An exploitable heap buffer overflow vulnerability exists in the iocheckd service ''I/O-Chec'' functionality of WAGO PFC 200 Firmware version 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a heap buffer overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5081**	N/A	O-WAG-PFC_-060120/2197
Xerox					
altalink_c8035_firmware					
Cross-Site Request Forgery (CSRF)	18-12-2019	6.8	Xerox AltaLink C8035 printers allow CSRF. A request to add users is made in the Device User Database form field to the xerox.set URI. (The frmUserName value must have a unique name.) **CVE ID : CVE-2019-19832**	N/A	O-XER-ALTA-060120/2198
Hardware					
Advantech					
diaganywhere_server					
Improper Restriction of Operations	17-12-2019	7.5	In Advantech DiagAnywhere Server, Versions 3.07.11 and prior, multiple stack-based buffer overflow	N/A	H-ADV-DIAG-060120/2199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			vulnerabilities exist in the file transfer service listening on the TCP port. Successful exploitation could allow an unauthenticated attacker to execute arbitrary code with the privileges of the user running DiagAnywhere Server. **CVE ID : CVE-2019-18257**		
Barco					
clickshare_button_r9861500d01					
Insufficiently Protected Credentials	17-12-2019	6.8	Barco ClickShare Button R9861500D01 devices before 1.9.0 have incorrect Credentials Management. The ClickShare Button implements encryption at rest which uses a one-time programmable (OTP) AES encryption key. This key is shared across all ClickShare Buttons of model R9861500D01. **CVE ID : CVE-2019-18832**	N/A	H-BAR-CLIC-060120/2200
Missing Encryption of Sensitive Data	17-12-2019	4.3	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information exposure (issue 2 of 2).. The encryption key of the media content which is shared between a ClickShare Button and a ClickShare Base Unit is randomly generated for each new session and communicated over a TLS connection. An attacker who is able to perform a Man-in-	N/A	H-BAR-CLIC-060120/2201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the-Middle attack between the TLS connection, is able to obtain the encryption key. **CVE ID : CVE-2019-18833**		
Improper Input Validation	17-12-2019	6.9	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Missing Support for Integrity Check. The ClickShare Button does not verify the integrity of the mutable content on the UBIFS partition before being used. **CVE ID : CVE-2019-18824**	N/A	H-BAR-CLIC-060120/2202
Untrusted Search Path	17-12-2019	4.4	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Missing Support for Integrity Check. The Barco signed 'Clickshare_For_Windows.exe' binary on the ClickShare Button (R9861500D01) loads a number of DLL files dynamically without verifying their integrity. **CVE ID : CVE-2019-18829**	N/A	H-BAR-CLIC-060120/2203
clickshare_cs-100_huddle					
N/A	17-12-2019	5	Barco ClickShare Huddle CS-100 devices before 1.9.0 and CSE-200 devices before 1.9.0 have incorrect Credentials Management. The ClickShare Base Unit implements encryption at rest using encryption keys which are shared across all ClickShare Base Units of models CS-100 & CSE-200.	N/A	H-BAR-CLIC-060120/2204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-18825		
clickshare_cse-200					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-12-2019	10	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow OS Command Injection. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, is vulnerable to OS command injection vulnerabilities. These vulnerabilities could lead to code execution on the ClickShare Button with the privileges of the user 'nobody'. **CVE ID : CVE-2019-18830**	N/A	H-BAR-CLIC-060120/2205
Information Exposure	16-12-2019	3.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information Exposure. The encrypted ClickShare Button firmware contains the private key of a test device-certificate. **CVE ID : CVE-2019-18831**	N/A	H-BAR-CLIC-060120/2206
N/A	17-12-2019	5	Barco ClickShare Huddle CS-100 devices before 1.9.0 and CSE-200 devices before 1.9.0 have incorrect Credentials Management. The ClickShare Base Unit implements encryption at rest using encryption keys which are shared across all ClickShare Base Units of models CS-100 & CSE-200.	N/A	H-BAR-CLIC-060120/2207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-18825		
Improper Certificate Validation	16-12-2019	7.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Improper Following of a Certificate's Chain of Trust. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, does not properly validate the whole certificate chain. **CVE ID : CVE-2019-18826**	N/A	H-BAR-CLIC-060120/2208
Improper Input Validation	16-12-2019	4.3	On Barco ClickShare Button R9861500D01 devices (before firmware version 1.9.0) JTAG access is disabled after ROM code execution. This means that JTAG access is possible when the system is running code from ROM before handing control over to embedded firmware. **CVE ID : CVE-2019-18827**	N/A	H-BAR-CLIC-060120/2209
Insufficiently Protected Credentials	16-12-2019	7.2	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Insufficiently Protected Credentials. The root account (present for access via debug interfaces, which are by default not enabled on production devices) of the embedded Linux on the ClickShare Button is using a weak password. **CVE ID : CVE-2019-18828**	N/A	H-BAR-CLIC-060120/2210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
clickshare_cs-100					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-12-2019	10	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow OS Command Injection. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, is vulnerable to OS command injection vulnerabilities. These vulnerabilities could lead to code execution on the ClickShare Button with the privileges of the user 'nobody'. **CVE ID : CVE-2019-18830**	N/A	H-BAR-CLIC-060120/2211
Information Exposure	16-12-2019	3.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information Exposure. The encrypted ClickShare Button firmware contains the private key of a test device-certificate. **CVE ID : CVE-2019-18831**	N/A	H-BAR-CLIC-060120/2212
Improper Certificate Validation	16-12-2019	7.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Improper Following of a Certificate's Chain of Trust. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, does not properly validate the whole certificate chain.	N/A	H-BAR-CLIC-060120/2213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-18826		
Improper Input Validation	16-12-2019	4.3	On Barco ClickShare Button R9861500D01 devices (before firmware version 1.9.0) JTAG access is disabled after ROM code execution. This means that JTAG access is possible when the system is running code from ROM before handing control over to embedded firmware. **CVE ID : CVE-2019-18827**	N/A	H-BAR-CLIC-060120/2214
Insufficiently Protected Credentials	16-12-2019	7.2	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Insufficiently Protected Credentials. The root account (present for access via debug interfaces, which are by default not enabled on production devices) of the embedded Linux on the ClickShare Button is using a weak password. **CVE ID : CVE-2019-18828**	N/A	H-BAR-CLIC-060120/2215
clickshare_cse-200\+					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-12-2019	10	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow OS Command Injection. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, is vulnerable to OS command injection vulnerabilities. These vulnerabilities could lead to	N/A	H-BAR-CLIC-060120/2216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution on the ClickShare Button with the privileges of the user 'nobody'. **CVE ID : CVE-2019-18830**		
Information Exposure	16-12-2019	3.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information Exposure. The encrypted ClickShare Button firmware contains the private key of a test device-certificate. **CVE ID : CVE-2019-18831**	N/A	H-BAR-CLIC-060120/2217
Improper Certificate Validation	16-12-2019	7.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Improper Following of a Certificate's Chain of Trust. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, does not properly validate the whole certificate chain. **CVE ID : CVE-2019-18826**	N/A	H-BAR-CLIC-060120/2218
Improper Input Validation	16-12-2019	4.3	On Barco ClickShare Button R9861500D01 devices (before firmware version 1.9.0) JTAG access is disabled after ROM code execution. This means that JTAG access is possible when the system is running code from ROM before handing control over to embedded firmware. **CVE ID : CVE-2019-18827**	N/A	H-BAR-CLIC-060120/2219

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	16-12-2019	7.2	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Insufficiently Protected Credentials. The root account (present for access via debug interfaces, which are by default not enabled on production devices) of the embedded Linux on the ClickShare Button is using a weak password. **CVE ID : CVE-2019-18828**	N/A	H-BAR-CLIC-060120/2220
clickshare_cse-800					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-12-2019	10	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow OS Command Injection. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, is vulnerable to OS command injection vulnerabilities. These vulnerabilities could lead to code execution on the ClickShare Button with the privileges of the user 'nobody'. **CVE ID : CVE-2019-18830**	N/A	H-BAR-CLIC-060120/2221
Information Exposure	16-12-2019	3.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information Exposure. The encrypted ClickShare Button firmware contains the private key of a test device-certificate.	N/A	H-BAR-CLIC-060120/2222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-18831		
Improper Certificate Validation	16-12-2019	7.5	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Improper Following of a Certificate's Chain of Trust. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to a USB host, does not properly validate the whole certificate chain. **CVE ID : CVE-2019-18826**	N/A	H-BAR-CLIC-060120/2223
Improper Input Validation	16-12-2019	4.3	On Barco ClickShare Button R9861500D01 devices (before firmware version 1.9.0) JTAG access is disabled after ROM code execution. This means that JTAG access is possible when the system is running code from ROM before handing control over to embedded firmware. **CVE ID : CVE-2019-18827**	N/A	H-BAR-CLIC-060120/2224
Insufficiently Protected Credentials	16-12-2019	7.2	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Insufficiently Protected Credentials. The root account (present for access via debug interfaces, which are by default not enabled on production devices) of the embedded Linux on the ClickShare Button is using a weak password. **CVE ID : CVE-2019-18828**	N/A	H-BAR-CLIC-060120/2225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dell					
xps_7390					
N/A	16-12-2019	7.2	Settings for the Dell XPS 13 2-in-1 (7390) BIOS versions prior to 1.1.3 contain a configuration vulnerability. The BIOS configuration for the "Enable Thunderbolt (and PCIe behind TBT) pre-boot modules" setting is enabled by default. A local unauthenticated attacker with physical access to a user's system can obtain read or write access to main memory via a DMA attack during platform boot. **CVE ID : CVE-2019-18579**	N/A	H-DEL-XPS_-060120/2226
Dlink					
dir-615_t1					
Improper Input Validation	16-12-2019	4	On D-Link DIR-615 devices, a normal user is able to create a root(admin) user from the D-Link portal. **CVE ID : CVE-2019-19743**	N/A	H-DLI-DIR--060120/2227
dir-615					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-12-2019	3.5	On D-Link DIR-615 devices, the User Account Configuration page is vulnerable to blind XSS via the name field. **CVE ID : CVE-2019-19742**	N/A	H-DLI-DIR--060120/2228
Huawei					
elle-al00b					
Buffer Copy	23-12-2019	5.8	Huawei smart phones with	https://ww	H-HUA-ELLE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			earlier versions than ELLE-AL00B 9.1.0.222(C00E220R2P1) have a buffer overflow vulnerability. An attacker may intercept and tamper with the packet in the local area network (LAN) to exploit this vulnerability. Successful exploitation may cause the affected phone abnormal. **CVE ID : CVE-2019-5276**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20191218-02-smartphone-en	060120/2229
oceanstor_sns3096					
Information Exposure	23-12-2019	2.1	Huawei OceanStor SNS3096 V100R002C01 have an information disclosure vulnerability. Attackers with low privilege can exploit this vulnerability by performing some specific operations. Successful exploit of this vulnerability can cause some information disclosure. **CVE ID : CVE-2019-5267**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191218-03-information-en	H-HUA-OCEA-060120/2230
p30					
Information Exposure	23-12-2019	5	Huawei Share function in P30 9.1.0.193(C00E190R2P1) smartphone has an improper access control vulnerability. The function incorrectly controls certain access messages, attackers can simulate a sender to steal P2P network information. Successful exploit may cause information leakage. **CVE ID : CVE-2019-5265**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191218-01-share-en	H-HUA-P30-060120/2231

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-12-2019	5	Huawei Share function in P30 9.1.0.193(C00E190R2P1) smartphone has an insufficient input validation vulnerability. Attackers can exploit this vulnerability by sending crafted packets to the affected device. Successful exploit may cause the function will be disabled. **CVE ID : CVE-2019-5266**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20191218-02-share-en	H-HUA-P30-060120/2232
humaxdigital					
hgb10r-2					
Cleartext Transmission of Sensitive Information	18-12-2019	5	An issue was discovered on Humax Wireless Voice Gateway HGB10R-2 20160817_1855 devices. The attacker can discover admin credentials in the backup file, aka backupsettings.conf. **CVE ID : CVE-2019-19889**	N/A	H-HUM-HGB1-060120/2233
Insufficiently Protected Credentials	18-12-2019	5	An issue was discovered on Humax Wireless Voice Gateway HGB10R-2 20160817_1855 devices. Admin credentials are sent over cleartext HTTP. **CVE ID : CVE-2019-19890**	N/A	H-HUM-HGB1-060120/2234
Qualcomm					
mdm9206					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MDM9-060120/2235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	lletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2238

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2240

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2241
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2243

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2245

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2246
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-MDM9-060120/2247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	mber-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2251
Out-of-	18-12-2019	7.5	Out of boundary access is	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MDM9-060120/2252
mdm9607					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-MDM9-060120/2253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2255

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2256
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2258

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2259

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2260

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2261
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon	https://www.qualcomm.com/company/produ	H-QUA-MDM9-060120/2262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	ct-security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2266
Out-of-	18-12-2019	10	Out-of-bound read in the	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MDM9-060120/2267
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2268

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2270
Buffer Copy without Checking Size of Input ('Classic	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that	https://www.qualcomm.com/company/product-	H-QUA-MDM9-060120/2271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2273
Buffer Copy without Checking Size of Input ('Classic Buffer	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MDM9-060120/2274

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 IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	lletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-060120/2276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
msm8909w					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2279

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10513		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2281
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto,	https://www.qualcomm.com/company/produ	H-QUA-MSM8-060120/2282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	ct-security/bulletins/december-2019-bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2286
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2292
msm8996au					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-MSM8-060120/2293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10482		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2297
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in	https://www.qualcomm.com/com	H-QUA-MSM8-060120/2298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MSM8-060120/2299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	lletins/december-2019-bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2300

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2302

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10536		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2304
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon	https://www.qualcomm.com/company/produ	H-QUA-MSM8-060120/2305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	ct-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2308
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-MSM8-060120/2309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	mber-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2311
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-060120/2314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
qca6574au					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA6-060120/2315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA6-060120/2316
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-QCA6-060120/2317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	bulletin	
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA6-060120/2318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA6-060120/2319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA6-060120/2320
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA6-060120/2321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA6-060120/2322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA6-060120/2323
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon	https://www.qualcomm.com/company/product-security/bu	H-QUA-QCA6-060120/2324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	lletins/december-2019-bulletin	
qcs405					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS4-060120/2325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS4-060120/2326
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto,	https://www.qualcomm.com/company/produ	H-QUA-QCS4-060120/2327

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	ct-security/bulletins/december-2019-bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS4-060120/2328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS4-060120/2329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS4-060120/2330
Improper Restriction of Operations within the	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in	https://www.qualcomm.com/company/product-	H-QUA-QCS4-060120/2331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS4-060120/2332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS4-060120/2333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS4-060120/2334
NULL	18-12-2019	7.2	Use of local variable as	https://ww	H-QUA-QCS4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/2335
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-QCS4-060120/2336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	mber-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS4-060120/2337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
qcs605					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2339
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2341

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2345
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2349
Improper	18-12-2019	4.6	Improper length check on	https://ww	H-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/2350
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-QCS6-060120/2351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	mber-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2352
Integer	18-12-2019	7.5	Improper check in video	https://ww	H-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/2353
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-QCS6-060120/2354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10600		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2357
Out-of-bounds	18-12-2019	7.5	Out of boundary access is possible as there is no	https://www.qualcom	H-QUA-QCS6-060120/2358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	m.com/company/product-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-QCS6-060120/2359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	bulletin	
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCS6-060120/2360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sda660					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2364
NULL Pointer	18-12-2019	4.9	Possibility of Null pointer access if the SPDM	https://www.qualcom	H-QUA-SDA6-060120/2365

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	m.com/company/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SDA6-060120/2366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	security/bulletins/december-2019-bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2371
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of	https://www.qualcomm.com/com	H-QUA-SDA6-060120/2372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	pany/product-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2375
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-SDA6-060120/2376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	mber-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2377
Buffer Copy without	18-12-2019	7.2	Out of bounds memcpy can occur by providing the	https://www.qualcom	H-QUA-SDA6-060120/2378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	m.com/company/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in	https://www.qualcomm.com/company/product-security/bu	H-QUA-SDA6-060120/2379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	lletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA6-060120/2381

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sdm439					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-060120/2382

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-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-060120/2383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-060120/2384
NULL	18-12-2019	4.9	Possibility of Null pointer	https://ww	H-QUA-SDM4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/2385
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in	https://www.qualcomm.com/company/produ	H-QUA-SDM4-060120/2386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	ct-security/bulletins/december-2019-bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-060120/2387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-060120/2388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-060120/2389

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-060120/2390
Integer	18-12-2019	7.5	Improper check in video	https://ww	H-QUA-SDM4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	060120/2391
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SDM4-060120/2392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-060120/2393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-060120/2394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-060120/2395

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-060120/2396
sdm630					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation	https://www.qualcomm.com/company/produ	H-QUA-SDM6-060120/2397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	ct-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-060120/2398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-060120/2399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-060120/2400

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-060120/2401

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-060120/2402

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-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-060120/2403
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-SDM6-060120/2404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	mber-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-060120/2405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-060120/2406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-060120/2407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-060120/2408
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in	https://www.qualcomm.com/company/product-	H-QUA-SDM6-060120/2409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-060120/2410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2412
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-SDM6-070120/2413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	mber-2019-bulletin	
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2415
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sdm660					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2420
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2425

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2426
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2428

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2430
Improper Restriction	18-12-2019	4.6	Improper length check on source buffer to handle	https://www.qualcom	H-QUA-SDM6-070120/2431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	m.com/company/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SDM6-070120/2432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2434
Improper Input	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack	https://www.qualcom	H-QUA-SDM6-070120/2435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	m.com/company/product-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2438
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2441
Improper Authenticati on	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto,	https://www.qualcomm.com/company/produ	H-QUA-SDM6-070120/2442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	ct-security/bulletins/december-2019-bulletin	
sdx20					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2445

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2447
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2452
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-SDX2-070120/2453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	mber-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2456
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2460
Integer Overflow or	18-12-2019	10	Device memory may get corrupted because of buffer	https://www.qualcom	H-QUA-SDX2-070120/2461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	m.com/company/product-security/bulletins/december-2019-bulletin	
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SDX2-070120/2462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	bulletin	
mdm9150					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2464

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2465

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2466

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2467

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2468
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MDM9-070120/2469

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	lletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2472

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
mdm9640					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2474
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer	https://www.qualcomm.com/com	H-QUA-MDM9-070120/2475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-MDM9-070120/2476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2478

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2480

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10572		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2482
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-MDM9-070120/2483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	mber-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2486

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
mdm9650					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2488
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison	https://www.qualcom	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/2489
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MDM9-070120/2490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	lletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10518		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2495
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another	https://www.qualcomm.com/com	H-QUA-MDM9-070120/2496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	pany/product-security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the Bounds of a	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MDM9-070120/2497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2500
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MDM9-070120/2501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	lletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10605		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2504
Out-of-bounds	18-12-2019	7.5	Out of boundary access is possible as there is no	https://www.qualcom	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/2505
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-MDM9-070120/2506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	bulletin	
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sdx24					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2509
Buffer Copy without Checking Size of Input ('Classic Buffer	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SDX2-070120/2510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	lletins/december-2019-bulletin	
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2514

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10525		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2517
Improper	18-12-2019	4.6	Improper length check on	https://ww	H-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	070120/2518
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-SDX2-070120/2519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	mber-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2522
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-SDX2-070120/2523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	mber-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2525
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SDX2-070120/2526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX2-070120/2527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
ipq4019					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ4-070120/2528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ4-070120/2529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ4-070120/2530
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ4-070120/2531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ4-070120/2532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ4-070120/2533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ4-070120/2534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ4-070120/2535
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ4-070120/2536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
ipq8064					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2304		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2538
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which	https://www.qualcomm.com/company/produ	H-QUA-IPQ8-070120/2539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	ct-security/bulletins/december-2019-bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2542
NULL	18-12-2019	7.2	Use of local variable as	https://ww	H-QUA-IPQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	070120/2543
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-IPQ8-070120/2544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	mber-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
ipq8074					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2546
Buffer Copy without Checking Size of Input ('Classic Buffer	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-IPQ8-070120/2547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	lletins/december-2019-bulletin	
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10518		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2551
NULL	18-12-2019	7.2	Use of local variable as	https://ww	H-QUA-IPQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	070120/2552
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-IPQ8-070120/2553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	mber-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-IPQ8-070120/2554
Buffer Copy without Checking Size of Input	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater	https://www.qualcomm.com/company/produ	H-QUA-IPQ8-070120/2555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	ct-security/bulletins/december-2019-bulletin	
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-IPQ8-070120/2556

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	bulletin	
qca6174a					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA6-070120/2557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA6-070120/2558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA6-070120/2559
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets	https://www.qualcomm.com/company/produ	H-QUA-QCA6-070120/2560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	ct-security/bulletins/december-2019-bulletin	
qca9377					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10557		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2564
qca9379					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-QCA9-070120/2565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	mber-2019-bulletin	
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2568
apq8009					
Incorrect Calculation	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen	https://www.qualcomm.com/com	H-QUA-APQ8-070120/2569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Buffer Size			due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	pany/product-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-APQ8-070120/2570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	bulletin	
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2572

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2574

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2575
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	H-QUA-APQ8-070120/2576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	lletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2580
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of	https://www.qualcomm.com/company/produ	H-QUA-APQ8-070120/2581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	ct-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2584
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead	https://www.qualcomm.com/company/produ	H-QUA-APQ8-070120/2585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	ct-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2589
apq8098					
Incorrect Calculation	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen	https://www.qualcomm.com/com	H-QUA-APQ8-070120/2590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Buffer Size			due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	pany/product-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-APQ8-070120/2591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	bulletin	
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2593

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2594

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2595

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2596
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	H-QUA-APQ8-070120/2597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	lletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2602

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2603
Buffer Copy without Checking Size of Input ('Classic Buffer	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-APQ8-070120/2604

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 IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	lletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
msm8939					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2609
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA	https://www.qualcom	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/2610
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-MSM8-070120/2611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	mber-2019-bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10525**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2615
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value	https://www.qualcomm.com/com	H-QUA-MSM8-070120/2616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	pany/product-security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2620
msm8953					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070120/2621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	security/bulletins/december-2019-bulletin	
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2624

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2629
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MSM8-070120/2630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	lletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2633
Out-of-bounds	18-12-2019	7.5	Out of boundary access is possible as there is no	https://www.qualcom	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/2634
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-MSM8-070120/2635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	bulletin	
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
msm8998					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2641
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MSM8-070120/2642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	lletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2648
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in	https://www.qualcomm.com/company/product-security/bu	H-QUA-MSM8-070120/2649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	lletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2651

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
nicobar					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2652

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-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2654
NULL	18-12-2019	4.9	Possibility of Null pointer	https://ww	H-QUA-NICO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	070120/2655
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in	https://www.qualcomm.com/company/produ	H-QUA-NICO-070120/2656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	ct-security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2660
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2664
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-NICO-070120/2667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
apq8053					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2669
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in	https://www.qualcomm.com/com	H-QUA-APQ8-070120/2670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-APQ8-070120/2671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	mber-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2674

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2676
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as	https://www.qualcomm.com/company/product-	H-QUA-APQ8-070120/2677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the Bounds of a Memory	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-APQ8-070120/2678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	bulletin	
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2680
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-APQ8-070120/2681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2684
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2688
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in	https://www.qualcomm.com/com	H-QUA-APQ8-070120/2689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	pany/product-security/bulletins/december-2019-bulletin	
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
mdm9207c					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2693
Use After	18-12-2019	4.6	Use after free of a pointer in	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MDM9-070120/2694
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-MDM9-070120/2695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	mber-2019-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2696

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2698
Out-of-	18-12-2019	4.6	Possibility of out of bound	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MDM9-070120/2699
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
msm8905					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10500		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2705
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA	https://www.qualcom	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/2706
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-MSM8-070120/2707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	mber-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2713
Integer	18-12-2019	10	Device memory may get	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MSM8-070120/2714
qcn7605					
Buffer Copy without Checking Size of Input ('Classic Buffer	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bu	H-QUA-QCN7-070120/2715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	lletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCN7-070120/2716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCN7-070120/2717
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-QCN7-070120/2718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	bulletin	
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCN7-070120/2719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCN7-070120/2720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCN7-070120/2721
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCN7-070120/2722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCN7-070120/2723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10598		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCN7-070120/2724
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCN7-070120/2725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCN7-070120/2726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10607		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCN7-070120/2727
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto,	https://www.qualcomm.com/company/produ	H-QUA-QCN7-070120/2728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	ct-security/bulletins/december-2019-bulletin	
sdm845					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2730

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2731
Information	18-12-2019	7.1	Due to the use of non-time-	https://ww	H-QUA-SDM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	070120/2732
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in	https://www.qualcomm.com/company/product-	H-QUA-SDM8-070120/2733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2736

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2738
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives	https://www.qualcom	H-QUA-SDM8-070120/2739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	m.com/company/product-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and	https://www.qualcomm.com/company/product-	H-QUA-SDM8-070120/2740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2742
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and	https://www.qualcomm.com/company/produ	H-QUA-SDM8-070120/2743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	ct-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2745

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2746
Improper Validation of	18-12-2019	7.2	Out of bound access can occur while processing	https://www.qualcom	H-QUA-SDM8-070120/2747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	m.com/company/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2748

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/2750
apq8017					
Incorrect Calculation	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen	https://www.qualcomm.com/com	H-QUA-APQ8-070120/2751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Buffer Size			due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	pany/product-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-APQ8-070120/2752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	bulletin	
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2754

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2755

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2756

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2757
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	H-QUA-APQ8-070120/2758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	lletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2762
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and	https://www.qualcomm.com/company/produ	H-QUA-APQ8-070120/2763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	ct-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2765

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2768
Improper	18-12-2019	7.2	Improper Access Control for	https://ww	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	070120/2769
apq8096au					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2773
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-	https://www.qualcomm.com/company/produ	H-QUA-APQ8-070120/2774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	ct-security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-APQ8-070120/2775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2777

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2779
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives	https://www.qualcom	H-QUA-APQ8-070120/2780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	m.com/company/product-security/bulletins/december-2019-bulletin	
Improper Restriction of Operations within the	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in	https://www.qualcomm.com/company/product-	H-QUA-APQ8-070120/2781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2784
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in	https://www.qualcomm.com/company/product-	H-QUA-APQ8-070120/2785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2787

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2788
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/2791

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
sda845					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2793
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2797

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2798

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2799
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2801

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2804
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10584		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2808
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDA8-070120/2812
sdm636					
Incorrect Calculation	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen	https://www.qualcomm.com/com	H-QUA-SDM6-070120/2813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Buffer Size			due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	pany/product-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SDM6-070120/2814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	bulletin	
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2816

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2817

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2818

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2819
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SDM6-070120/2820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	lletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2821

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2823

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2824
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and	https://www.qualcomm.com/company/produ	H-QUA-SDM6-070120/2825

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	ct-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2827

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2828
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SDM6-070120/2829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	lletins/december-2019-bulletin	
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2831
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sdm670					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2836
Information	18-12-2019	7.1	Due to the use of non-time-	https://ww	H-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	070120/2837
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in	https://www.qualcomm.com/company/product-	H-QUA-SDM6-070120/2838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2840

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2843

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2844

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2845
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2848

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10614		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/2850
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-SDM6-070120/2851

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 APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	security/bulletins/december-2019-bulletin	
sdm710					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2853

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2855

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2857
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during	https://www.qualcom	H-QUA-SDM7-070120/2858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	m.com/company/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SDM7-070120/2859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	bulletin	
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2863
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted	https://www.qualcomm.com/com	H-QUA-SDM7-070120/2864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	pany/product-security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2867

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authenticati on	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM7-070120/2868

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca8081					
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA8-070120/2869
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA8-070120/2870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA8-070120/2871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA8-070120/2872

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA8-070120/2873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA8-070120/2874
qcs404					
Information	18-12-2019	7.1	Due to the use of non-time-constant comparison	https://www.qualcom	H-QUA-QCS4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/2875
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-QCS4-070120/2876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	lletins/december-2019-bulletin	
sxr1130					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-SXR1-070120/2877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	mber-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10482		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2881
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in	https://www.qualcomm.com/com	H-QUA-SXR1-070120/2882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SXR1-070120/2883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	lletins/december-2019-bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2884

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10536		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2888
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2890
Out-of-	18-12-2019	4.6	Possible OOB issue in	https://ww	H-QUA-SXR1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	070120/2891
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2892

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2894
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2896

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2898

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR1-070120/2899
sm6150					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2900
Buffer Copy without Checking Size of Input ('Classic Buffer	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bu	H-QUA-SM61-070120/2901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	lletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2903
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SM61-070120/2904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2905

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2907

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10517		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2909
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last	https://www.qualcomm.com/company/produ	H-QUA-SM61-070120/2910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	ct-security/bulletins/december-2019-bulletin	
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SM61-070120/2911

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, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	bulletin	
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2912

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2914
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2916

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2917
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope	https://www.qualcomm.com/com	H-QUA-SM61-070120/2918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	pany/product-security/bulletins/december-2019-bulletin	
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SM61-070120/2919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM61-070120/2922
sm8150					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2926
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2928

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2930

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2931
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SM81-070120/2932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10537		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2936
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of	https://www.qualcomm.com/company/produ	H-QUA-SM81-070120/2937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	ct-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2940
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM81-070120/2944
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bu	H-QUA-SM81-070120/2945

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 APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	lletins/december-2019-bulletin	
mdm9615					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2947

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2948

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10595		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2950
Integer Overflow or	18-12-2019	10	Device memory may get corrupted because of buffer	https://www.qualcom	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/2951
mdm9625					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-MDM9-070120/2952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	mber-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2954

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2956

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
mdm9205					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10500		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2958
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA	https://www.qualcom	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/2959
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-MDM9-070120/2960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	mber-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
msm8909					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2965

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2967
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent	https://www.qualcom	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/2968
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2972
NULL Pointer	18-12-2019	7.2	Use of local variable as argument to netlink CB	https://www.qualcom	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/2973
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-MSM8-070120/2974

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 APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10605**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2975

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/2976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
mdm9655					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2977

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2978
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-MDM9-070120/2979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
mdm9635m					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2984
Out-of-	18-12-2019	10	Multiple read overflows in	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MDM9-070120/2985
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-MDM9-070120/2986

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	mber-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/2987

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
qca9531					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
qca9880					
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
qca9886					
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10607		
qca9980					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2992
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value	https://www.qualcomm.com/com	H-QUA-QCA9-070120/2993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	pany/product-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/2994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
qm215					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QM21-070120/2995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QM21-070120/2996

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QM21-070120/2997

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QM21-070120/2998

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QM21-070120/2999

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-10516**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QM21-070120/3000
Improper Restriction	18-12-2019	4.6	Improper length check on source buffer to handle	https://www.qualcom	H-QUA-QM21-070120/3001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	m.com/company/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-QM21-070120/3002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QM21-070120/3003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QM21-070120/3004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QM21-070120/3005
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed	https://www.qualcomm.com/com	H-QUA-QM21-070120/3006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	pany/product-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-QM21-070120/3007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	bulletin	
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QM21-070120/3008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sm7150					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3010
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-SM71-070120/3011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	mber-2019-bulletin	
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3015
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach	https://www.qualcomm.com/com	H-QUA-SM71-070120/3016

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	pany/product-security/bulletins/december-2019-bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SM71-070120/3017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3019

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-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3021
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3024
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if	https://www.qualcom	H-QUA-SM71-070120/3025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	m.com/company/product-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10601**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3028
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM71-070120/3031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
sdm429					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3033
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-	https://www.qualcomm.com/company/produ	H-QUA-SDM4-070120/3034

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	ct-security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SDM4-070120/3035

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3040
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3045
Improper Authenticati	18-12-2019	7.2	Improper Access Control for RPU write access from	https://www.qualcom	H-QUA-SDM4-070120/3046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	m.com/company/product-security/bulletins/december-2019-bulletin	
sdm632					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/3047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/3048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/3049

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/3050

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/3051

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/3052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10518		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/3053
Improper Restriction of	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can	https://www.qualcomm.com/com	H-QUA-SDM6-070120/3054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SDM6-070120/3055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/3056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/3057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10584		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/3058
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of	https://www.qualcomm.com/company/produ	H-QUA-SDM6-070120/3059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	ct-security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM6-070120/3060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authenticati on	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655,	https://ww w.qualcom m.com/com pany/produ ct-security/bu lletins/dece mber-2019-bulletin	H-QUA-SDM6-070120/3061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**		
msm8917					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3063
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-MSM8-070120/3064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	bulletin	
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3065

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3066

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3068

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3069
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070120/3070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	security/bulletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3072

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3073

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10564		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3075
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070120/3076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3078

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3080

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3081
msm8920					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070120/3082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3086
NULL Pointer	18-12-2019	4.9	Possibility of Null pointer access if the SPDM	https://www.qualcom	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/3087
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070120/3088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	security/bulletins/december-2019-bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3091

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3093
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can	https://www.qualcomm.com/com	H-QUA-MSM8-070120/3094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3096

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3097

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3100
msm8937					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3104
Out-of-	18-12-2019	10	Buffer over read can happen	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MSM8-070120/3105
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MSM8-070120/3106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	lletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-MSM8-070120/3107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10525		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3111
Improper	18-12-2019	4.6	Improper length check on	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MSM8-070120/3112
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-MSM8-070120/3113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	mber-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3118
Improper Authenticati on	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto,	https://www.qualcomm.com/company/produ	H-QUA-MSM8-070120/3119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	ct-security/bulletins/december-2019-bulletin	
msm8940					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3121

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10480**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3122
Information	18-12-2019	7.1	Due to the use of non-time-	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MSM8-070120/3123
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070120/3124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3126

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3127

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10518**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3129
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives	https://www.qualcom	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/3130
Improper Restriction of Operations within the	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070120/3131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	security/bulletins/december-2019-bulletin	
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3133

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3134

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3135

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3136
Integer	18-12-2019	10	Device memory may get	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	MSM8-070120/3137
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-MSM8-070120/3138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	bulletin	
msm8996					
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MSM8-070120/3141

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
sdm450					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3144

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10487		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3145
Out-of-	18-12-2019	10	Multiple read overflows in	https://ww	H-QUA-SDM4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	070120/3146
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-SDM4-070120/3147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	mber-2019-bulletin	
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3151
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if	https://www.qualcom	H-QUA-SDM4-070120/3152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	m.com/company/product-security/bulletins/december-2019-bulletin	
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM4-070120/3156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2274		
sm8250					
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM82-070120/3157
Double Free	18-12-2019	4.6	Memory is being freed up	https://ww	H-QUA-SM82-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	w.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	070120/3158
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM82-070120/3159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM82-070120/3160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM82-070120/3161
Improper Restriction	18-12-2019	4.6	Improper length check on source buffer to handle	https://www.qualcom	H-QUA-SM82-070120/3162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	m.com/company/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SM82-070120/3163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**	bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM82-070120/3164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM82-070120/3165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SM82-070120/3166
sxr2130					
Information	18-12-2019	7.1	Due to the use of non-time-constant comparison	https://www.qualcom	H-QUA-SXR2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/3167
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SXR2-070120/3168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	lletins/december-2019-bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SXR2-070120/3169

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**	bulletin	
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR2-070120/3170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR2-070120/3171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10537**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR2-070120/3172
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR2-070120/3173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR2-070120/3174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR2-070120/3175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10584		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SXR2-070120/3176
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of	https://www.qualcomm.com/company/produ	H-QUA-SXR2-070120/3177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	ct-security/bulletins/december-2019-bulletin	
apq8016					
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-APQ8-070120/3178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**	bulletin	
sa6155p					
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SA61-070120/3179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SA61-070120/3180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SA61-070120/3181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**		
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SA61-070120/3182
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SA61-070120/3183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**	lletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SA61-070120/3184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**		
sc8180x					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SC81-070120/3185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SC81-070120/3186

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SC81-070120/3187

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SC81-070120/3188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SC81-070120/3189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdm850					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/3190
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which	https://www.qualcomm.com/company/produ	H-QUA-SDM8-070120/3191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**	ct-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-SDM8-070120/3192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	bulletin	
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/3193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**		
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/3194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/3195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/3196

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDM8-070120/3197
qcm2150					
Incorrect Calculation	18-12-2019	10	While processing MT Secondary PDP request,	https://www.qualcom	H-QUA-QCM2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Buffer Size			Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/3198
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-	H-QUA-QCM2-070120/3199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCM2-070120/3200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCM2-070120/3201

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCM2-070120/3202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
sdx55					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3203

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-2019-10500**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2304**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3204
Improper Validation of Array Index	18-12-2019	7.2	Out of bound access occurs while handling the WMI FW event due to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150 **CVE ID : CVE-2019-10481**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10482**		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**		
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3209
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SDX5-070120/3210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**	lletins/december-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Double Free	18-12-2019	7.2	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10536**		
Integer Overflow or Wraparound	18-12-2019	7.2	Improper validation of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2019-10537**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	4.6	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10544**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3214
Out-of-bounds Read	18-12-2019	10	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of	https://www.qualcomm.com/com	H-QUA-SDX5-070120/3215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130 **CVE ID : CVE-2019-10557**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	4.6	Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2019-10564**		
Integer Overflow or Wraparound	18-12-2019	7.5	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10572**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3217
Out-of-bounds Read	18-12-2019	4.6	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto,	https://www.qualcomm.com/company/produ	H-QUA-SDX5-070120/3218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10584**	ct-security/bulletins/december-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10598**		
NULL Pointer Dereference	18-12-2019	7.2	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3220

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10600**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10607		
Out-of-bounds Write	18-12-2019	7.5	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10614**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-SDX5-070120/3222
Improper Authentication	18-12-2019	7.2	Improper Access Control for RPU write access from secure processor in Snapdragon Auto,	https://www.qualcomm.com/company/produ	H-QUA-SDX5-070120/3223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-2274**	ct-security/bulletins/december-2019-bulletin	
apq8064					
Use After Free	18-12-2019	4.6	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/3224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10518**		
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/3225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/3226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
apq8096					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/3227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**		
Information Exposure	18-12-2019	7.1	Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/3228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10482		
Out-of-bounds Read	18-12-2019	10	Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/3229
NULL Pointer Dereference	18-12-2019	4.9	Possibility of Null pointer access if the SPDM commands are executed in	https://www.qualcomm.com/com	H-QUA-APQ8-070120/3230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the non-standard way in Trustzone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 **CVE ID : CVE-2019-10513**	pany/product-security/bulletins/december-2019-bulletin	
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-APQ8-070120/3231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	lletins/december-2019-bulletin	
Double Free	18-12-2019	4.6	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/3232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2019-10517**		
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/3233

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-APQ8-070120/3234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
mdm9645					
Incorrect Calculation of Buffer Size	18-12-2019	10	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10500**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/3235
Out-of-	18-12-2019	10	Buffer over read can happen while parsing SMS OTA	https://www.qualcom	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			messages at transport layer if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10487**	m.com/company/product-security/bulletins/december-2019-bulletin	070120/3236
Out-of-bounds Read	18-12-2019	10	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/dece	H-QUA-MDM9-070120/3237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10516**	mber-2019-bulletin	
Out-of-bounds Write	18-12-2019	10	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/3238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2019-10525**		
Integer Overflow or Wraparound	18-12-2019	10	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-MDM9-070120/3239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130 **CVE ID : CVE-2019-2242**		
qca4531					
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA4-070120/3240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980,	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA4-070120/3241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**		
qca9558					
Improper Input Validation	18-12-2019	7.2	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10595**	https://www.qualcomm.com/company/product-security/bulletins/december-2019-bulletin	H-QUA-QCA9-070120/3242
Buffer Copy without Checking Size of Input	18-12-2019	7.2	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater	https://www.qualcomm.com/company/produ	H-QUA-QCA9-070120/3243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2019-10607**	ct-security/bulletins/december-2019-bulletin	
Sonicwall					
sma_100					
Information Exposure	17-12-2019	5	Vulnerability in SonicWall SMA100 allow unauthenticated user to gain read-only access to unauthorized resources.	https://psirt.global.sonicwall.com/vuln-detail/SNW	H-SON-SMA_-070120/3244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This vulnerablity impacted SMA100 version 9.0.0.3 and earlier. **CVE ID : CVE-2019-7481**	LID-2019-0016	
Trendnet					
tew-651br					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-12-2019	10	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. OS command injection occurs through the get_set.ccp lanHostCfg_HostName_1.1.1.0.0 parameter. **CVE ID : CVE-2019-11399**	N/A	H-TRE-TEW--070120/3245
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. A buffer overflow occurs through the get_set.ccp ccp_act parameter. **CVE ID : CVE-2019-11400**	N/A	H-TRE-TEW--070120/3246
tew-652bru					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-12-2019	10	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. OS command injection occurs through the get_set.ccp lanHostCfg_HostName_1.1.1.0.0 parameter. **CVE ID : CVE-2019-11399**	N/A	H-TRE-TEW--070120/3247
Improper Restriction	18-12-2019	7.5	An issue was discovered on TRENDnet TEW-651BR	N/A	H-TRE-TEW--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. A buffer overflow occurs through the get_set.ccp ccp_act parameter. **CVE ID : CVE-2019-11400**		070120/3248
tew-652brp					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-12-2019	10	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. OS command injection occurs through the get_set.ccp lanHostCfg_HostName_1.1.1.0.0 parameter. **CVE ID : CVE-2019-11399**	N/A	H-TRE-TEW--070120/3249
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	7.5	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. A buffer overflow occurs through the get_set.ccp ccp_act parameter. **CVE ID : CVE-2019-11400**	N/A	H-TRE-TEW--070120/3250
Wago					
pfc_200					
Information Exposure	18-12-2019	5	An exploitable information exposure vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially	N/A	H-WAG-PFC_-070120/3251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted set of packets can cause an external tool to fail, resulting in uninitialized stack data to be copied to the response packet buffer. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5073**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	10	An exploitable stack buffer overflow vulnerability exists in the iocheckd service ''I/O-Check'' functionality of WAGO PFC200 Firmware version 03.01.07(13), WAGO PFC200 Firmware version 03.00.39(12) and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a stack buffer overflow, resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5074**	https://talosintelligence.com/vulnerability_reports/TALOS-2019-0863	H-WAG-PFC_-070120/3252
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	10	An exploitable stack buffer overflow vulnerability exists in the command line utility getcouplerdetails of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets sent to the iocheckd service "I/O-Check" can cause a stack buffer overflow in the sub-	N/A	H-WAG-PFC_-070120/3253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process getcouplerdetails, resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5075**		
Missing Authenticati on for Critical Function	18-12-2019	8.5	An exploitable denial-of-service vulnerability exists in the iocheckd service ??I/O-Chec?? functionality of WAGO PFC 200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC 100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a denial of service, resulting in the device entering an error state where it ceases all network communications. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5077**	N/A	H-WAG-PFC_-070120/3254
Missing Authenticati on for Critical Function	18-12-2019	9.4	An exploitable denial of service vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a denial of service, resulting in the device entering an error state where it ceases all network communications. An attacker	N/A	H-WAG-PFC_-070120/3255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5078**		
Out-of-bounds Write	18-12-2019	7.5	An exploitable heap buffer overflow vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a heap buffer overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5079**	N/A	H-WAG-PFC_-070120/3256
Missing Authentication for Critical Function	18-12-2019	6.4	An exploitable denial-of-service vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC 200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A single packet can cause a denial of service and weaken credentials resulting in the default documented credentials being applied to the device. An attacker can send an unauthenticated packet to trigger this vulnerability.	N/A	H-WAG-PFC_-070120/3257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5080		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	10	An exploitable heap buffer overflow vulnerability exists in the iocheckd service ''I/O-Chec'' functionality of WAGO PFC 200 Firmware version 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a heap buffer overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5081**	N/A	H-WAG-PFC_-070120/3258
pfc_100					
Information Exposure	18-12-2019	5	An exploitable information exposure vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause an external tool to fail, resulting in uninitialized stack data to be copied to the response packet buffer. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5073**	N/A	H-WAG-PFC_-070120/3259
Buffer Copy without	18-12-2019	10	An exploitable stack buffer overflow vulnerability exists	https://talosintelligenc	H-WAG-PFC_-070120/3260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			in the iocheckd service ''I/O-Check'' functionality of WAGO PFC200 Firmware version 03.01.07(13), WAGO PFC200 Firmware version 03.00.39(12) and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a stack buffer overflow, resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5074**	e.com/vulnerability_reports/TALOS-2019-0863	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-12-2019	10	An exploitable stack buffer overflow vulnerability exists in the command line utility getcouplerdetails of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets sent to the iocheckd service "I/O-Check" can cause a stack buffer overflow in the sub-process getcouplerdetails, resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5075**	N/A	H-WAG-PFC_-070120/3261
Missing Authentication for Critical Function	18-12-2019	8.5	An exploitable denial-of-service vulnerability exists in the iocheckd service ??I/O-Chec?? functionality of WAGO PFC 200 Firmware	N/A	H-WAG-PFC_-070120/3262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions 03.01.07(13) and 03.00.39(12), and WAGO PFC 100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a denial of service, resulting in the device entering an error state where it ceases all network communications. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5077**		
Missing Authenticati on for Critical Function	18-12-2019	9.4	An exploitable denial of service vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a denial of service, resulting in the device entering an error state where it ceases all network communications. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5078**	N/A	H-WAG-PFC_-070120/3263
Out-of-bounds Write	18-12-2019	7.5	An exploitable heap buffer overflow vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO	N/A	H-WAG-PFC_-070120/3264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a heap buffer overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5079**		
Missing Authenticati on for Critical Function	18-12-2019	6.4	An exploitable denial-of-service vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC 200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A single packet can cause a denial of service and weaken credentials resulting in the default documented credentials being applied to the device. An attacker can send an unauthenticated packet to trigger this vulnerability. **CVE ID : CVE-2019-5080**	N/A	H-WAG-PFC_-070120/3265
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-12-2019	10	An exploitable heap buffer overflow vulnerability exists in the iocheckd service ''I/O-Chec'' functionality of WAGO PFC 200 Firmware version 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a heap buffer	N/A	H-WAG-PFC_-070120/3266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability. **CVE ID : CVE-2019-5081**		
Xerox					
altalink_c8035					
Cross-Site Request Forgery (CSRF)	18-12-2019	6.8	Xerox AltaLink C8035 printers allow CSRF. A request to add users is made in the Device User Database form field to the xerox.set URI. (The frmUserName value must have a unique name.) **CVE ID : CVE-2019-19832**	N/A	H-XER-ALTA-070120/3267