

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

## National Critical Information Infrastructure Protection Centre Common Vulnerabilities and Exposures(CVE) Report

16 - 30 Nov 2019

Vol. 06 No. 22

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Application		
Apache					
atlas					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-11-2019	4.3	Apache Atlas versions 0.8.3 and 1.1.0 were found vulnerable to Stored Cross-Site Scripting in the search functionality  CVE ID: CVE-2019-10070	N/A	A-APA-ATLA- 031219/1
nifi					
Improper Restriction of XML External Entity Reference ('XXE')	19-11-2019	4	The XMLFileLookupService in NiFi versions 1.3.0 to 1.9.2 allowed trusted users to inadvertently configure a potentially malicious XML file. The XML file has the ability to make external calls to services (via XXE) and reveal information such as the versions of Java, Jersey, and Apache that the NiFI instance uses.  CVE ID: CVE-2019-10080	https://nifi. apache.org/ security.ht ml#CVE- 2019- 10080	A-APA-NIFI- 031219/2
Information Exposure	19-11-2019	5	When updating a Process Group via the API in NiFi versions 1.3.0 to 1.9.2, the response to the request includes all of its contents (at the top most level, not recursively). The response included details about processors and controller	https://nifi. apache.org/ security.ht ml#CVE- 2019- 10083	A-APA-NIFI- 031219/3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	CID
			services which the user may not have had read access to.							
			CVE ID : CVE-2019-10083							
Insufficient Session Expiration	19-11-2019	6.5	When using an authentication mechanism other than PKI, when the user clicks Log Out in NiFi versions 1.0.0 to 1.9.2, NiFi invalidates the authentication token on the client side but not on the server side. This permits the user's client-side token to be used for up to 12 hours after logging out to make API requests to NiFi.  CVE ID: CVE-2019-12421				https:/apachesecuritml#CV 2019-	e.org/ ty.ht 'E-	A-APA-N 031219,	
solr			CVE	CVE ID : CVE-2019-12421						
Unrestricted Upload of File with Dangerous Type	18-11-2019	7.5	of Apa insect ENAB S config defau config with S defau the af JMX n enable witho If this inbour fireway networe nodes JMX, v allow	The 8.1.1 and 8.2.0 releases of Apache Solr contain an insecure setting for the ENABLE_REMOTE_JMX_OPT S configuration option in the default solr.in.sh configuration file shipping with Solr. If you use the default solr.in.sh file from the affected releases, then JMX monitoring will be enabled and exposed on RMI_PORT (default=18983), without any authentication. If this port is opened for inbound traffic in your firewall, then anyone with network access to your Solr nodes will be able to access JMX, which may in turn allow them to upload malicious code for execution		N/A		A-APA-S 031219	_	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on the Solr server.		
			CVE ID : CVE-2019-12409		
shiro					
Improper Input Validation	18-11-2019	5	Apache Shiro before 1.4.2, when using the default "remember me" configuration, cookies could be susceptible to a padding attack.  CVE ID: CVE-2019-12422	N/A	A-APA-SHIR- 031219/6
Cantraga			CVE ID . CVE-2019-12422		
Centreon					
centreon_web	)			T	
Incorrect Permission Assignment for Critical Resource	21-11-2019	7.2	Centreon Web 19.04.4 has weak permissions within the OVA (aka VMware virtual machine) and OVF (aka VirtualBox virtual machine) files, allowing attackers to gain privileges via a Trojan horse Centreon-autodisco executable file that is launched by cron.	N/A	A-CEN-CENT- 031219/7
			CVE ID : CVE-2019-16406		
cloudfoundry					
cf-deploymen	it				
Improper Input Validation	19-11-2019	7.8	Cloud Foundry Routing, all versions before 0.193.0, does not properly validate nonce input. A remote unauthorized malicious user could forge a route service request using an invalid nonce that will cause the Gorouter to crash.  CVE ID: CVE-2019-11289	https://ww w.cloudfou ndry.org/bl og/cve- 2019- 11289	A-CLO-CF-D- 031219/8
routing-relea	se				

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	19-11-2019	7.8	Cloud Foundry Routing, all versions before 0.193.0, does not properly validate nonce input. A remote unauthorized malicious user could forge a route service request using an invalid nonce that will cause the Gorouter to crash.  CVE ID: CVE-2019-11289	https://ww w.cloudfou ndry.org/bl og/cve- 2019- 11289	A-CLO-ROUT- 031219/9
code42					
code42					
Untrusted Search Path	19-11-2019	6.9	Code42 app through version 7.0.2 for Windows has an Untrusted Search Path. In certain situations, a nonadministrative attacker on the local machine could create or modify a dynamiclink library (DLL). The Code42 service could then load it at runtime, and potentially execute arbitrary code at an elevated privilege on the local machine.  CVE ID: CVE-2019-16860	https://sup port.code42 .com/Term s_and_condi tions/Code 42_custome r_support_r esources/C ode42_secu rity_advisor ies/Arbitrar y_code_exec ution_on_lo cal_Window s_devices	A-COD-CODE- 031219/10
Untrusted Search Path	19-11-2019	6.9	Code42 server through 7.0.2 for Windows has an Untrusted Search Path. In certain situations, a nonadministrative attacker on the local server could create or modify a dynamic-link library (DLL). The Code42 service could then load it at runtime, and potentially execute arbitrary code at an elevated privilege on the	https://cod e42.com/r/ support/CV E-2019- 16861	A-COD-CODE- 031219/11

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			local server.		
			CVE ID : CVE-2019-16861		
Codesys					
control_for_p	lcnext				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.  CVE ID: CVE-2019-18858	N/A	A-COD-CONT- 031219/12
control_for_b	eaglebone				1
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.  CVE ID: CVE-2019-18858	N/A	A-COD-CONT- 031219/13
control_for_e	mpc-a\/imx6				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.  CVE ID: CVE-2019-18858	N/A	A-COD-CONT- 031219/14
control_for_io	t2000				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.  CVE ID: CVE-2019-18858	N/A	A-COD-CONT- 031219/15
control_for_li	nux				
Buffer Copy	20-11-2019	7.5	CODESYS 3 web server	N/A	A-COD-CONT-
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
without Checking Size of Input ('Classic Buffer Overflow')			before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.  CVE ID: CVE-2019-18858						031219	/16
control_for_p	fc100									
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	before distri Contr has a	SYS 3 we as 3.5.15. buted we old runting Buffer O cve-	20, as ith CODI ne syste verflow	ESYS ms,	N/A		A-COD-031219	
control_for_p	fc200									
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	before distri Contr has a	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.  CVE ID: CVE-2019-18858					A-COD-0 031219	
control_for_ra	aspberry_pi									
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	before distri Contr has a	SYS 3 we as 3.5.15. buted we old runting Buffer O	20, as ith CODI ne syste verflow	ESYS ms,	N/A		A-COD-031219	
control_rte										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.  CVE ID: CVE-2019-18858				N/A		A-COD-0 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	<b>2-3</b> 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
control_runti	me_system_to	olkit								
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	before distrik Contro has a	e 3.5.15. outed war ol runtir Buffer O	eb serve 20, as ith CODI ne syste verflow <b>2019-1</b>	ESYS ems,	N/A		A-COD- 031219	
control_win										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	before distrik Contro has a	e 3.5.15. outed war ol runtin Buffer O	eb serve 20, as ith CODI ne syste verflow <b>2019-1</b>	ESYS ems,	N/A		A-COD- 031219	
embedded_ta	rget_visu_too	lkit								
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	before distrik Contro has a	e 3.5.15. outed war ol runtir Buffer O	eb serve 20, as ith CODI ne syste verflow <b>2019-1</b>	ESYS ems,	N/A		A-COD- 031219	
hmi										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	before distrib Contro has a	e 3.5.15. outed wool ol runtir Buffer O	eb serve 20, as ith CODI ne syste verflow <b>2019-1</b>	ESYS ems,	N/A		A-COD- 031219	
remote_targe	t_visu_toolkit									
Buffer Copy without Checking Size of Input ('Classic	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.					A-COD- 031219		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	tch	NCIII	PC ID
Buffer			CVE I	D : CVE-	2019-1	8858				
Overflow')										
Comodo										
comodo_inter	net_security									
Untrusted Search Path	18-11-2019	4.4	An issue was discovered in signmgr.dll 6.5.0.819 in Comodo Internet Security through 12.0. A DLL Preloading vulnerability allows an attacker to implant an unsigned DLL named iLog.dll in a partially unprotected product directory. This DLL is then loaded into a high-privileged service before the binary signature validation logic is loaded, and might bypass some of the self-defense mechanisms.  CVE ID: CVE-2019-18215				N/A		A-COM COMO- 031219	
Fasterxml										
jackson-mapj	per-asl									
Improper Restriction of XML External Entity Reference ('XXE')	18-11-2019	5	org.co n-map XML e vulne 2016- codeh asl lib classe	A flaw was found in org.codehaus.jackson:jackson-mapper-asl:1.9.x libraries. XML external entity vulnerabilities similar CVE-2016-3720 also affects codehaus jackson-mapper-asl libraries but in different classes.  CVE ID: CVE-2019-10172				//bug edhat. how_ i?id= 019-	A-FAS-) 031219	
footy										
tipping_softw	are									
Improper Neutralizatio n of Input	18-11-2019	4.3	Footy Tipping Software AFL Web Edition 2019 allows			N/A		A-F00- 031219		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			XSS.  CVE ID : CVE-2019-17057		
Unrestricted Upload of File with Dangerous Type	18-11-2019	6.5	Footy Tipping Software AFL Web Edition 2019 allows arbitrary file upload and resultant remote code execution because a whitelist can be bypassed by an Administrator who uploads a crafted upload.dat file.  CVE ID: CVE-2019-17058	N/A	A-F00-TIPP- 031219/29
Fortinet					
forticlient					
Information Exposure	21-11-2019	2.1	A clear text storage of sensitive information vulnerability in FortiClient for Mac may allow a local attacker to read sensitive information logged in the console window when the user connects to an SSL VPN Gateway.  CVE ID: CVE-2019-15704	https://fort iguard.com /advisory/F G-IR-19- 227	A-FOR-FORT- 031219/30
getmailbird					
mailbird					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-11-2019	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Mailbird before 2.7.5.0 r allow remote attackers to execute arbitrary JavaScript in a privileged context via a crafted HTML mail message. This vulnerability is distinct from CVE-2015-4657.	https://ww w.getmailbi rd.com/Rel easeNotes/ LatestRelea seNotes.ht ml	A-GET-MAIL- 031219/31
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIII	PC ID
			CVE I	D : CVE-	2019-1	5054				
GNU							L			
serveez										
Information Exposure	20-11-2019	5	GNU Serveez through 0.2.2 has an Information Leak. An attacker may send an HTTP POST request to the /cgibin/reader URI. The attacker must include a Contentlength header with a large positive value that, when represented in 32 bit binary, evaluates to a negative number. The problem exists in the http_cgi_write function under http-cgi.c; however, exploitation might show svz_envblock_add in libserveez/passthrough.c as the location of the heapbased buffer over-read.				N/A		A-GNU- 031219	
Google										
chrome										
Use After Free	25-11-2019	4.3	Use after free in PDFium in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.			N/A		A-G00- 031219		
Use After Free	25-11-2019	4.3	Use after free in PDFium in Google Chrome prior to 76.0.3809.100 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF				N/A		A-G00- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file.  CVE ID : CVE-2019-5868		
Use After Free	25-11-2019	4.3	Use after free in Blink in Google Chrome prior to 76.0.3809.132 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-5869	N/A	A-GOO-CHRO- 031219/35
Use After Free	25-11-2019	6.8	Use after free in media in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.  CVE ID: CVE-2019-5870	N/A	A-GOO-CHRO- 031219/36
Use After Free	25-11-2019	4.3	Use after free in Mojo in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-5872	N/A	A-GOO-CHRO- 031219/37
Use After Free	25-11-2019	6.8	Use after free in media in Google Chrome on Android prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-5876	N/A	A-G00-CHR0- 031219/38
Use After Free	25-11-2019	6.8	Use after free in V8 in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to	N/A	A-G00-CHR0- 031219/39
CV Scoring Scal (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			corru HTMI	tially ex ption via _ page. <b>D : CVE-</b>	a crafte	ed				
Use After Free	25-11-2019	6.8	Use at view to 77. remo poten corru	Use after free in sharing view in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-13685  Use after free in offline mode					A-G00-0 031219	
Use After Free	25-11-2019	6.8	Use after free in offline mode in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-13686				N/A		A-GOO-0 031219	
Use After Free	25-11-2019	6.8	Googl 77.0.3 remo poten corru HTMI	Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-13687		N/A		A-G00-031219		
Use After Free	25-11-2019	6.8	Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-13688			N/A		A-GOO-CHRO- 031219/43		
Use After Free	25-11-2019	6.8	Use after free in IndexedDB in Google Chrome prior to			N/A		A-G00-0		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			77.0.3865.120 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.  CVE ID: CVE-2019-13693		
Use After Free	25-11-2019	6.8	Use after free in WebRTC in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-13694	N/A	A-G00-CHR0- 031219/45
Use After Free	25-11-2019	6.8	Use after free in audio in Google Chrome on Android prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-13695	N/A	A-G00-CHR0- 031219/46
Use After Free	25-11-2019	6.8	Use after free in JavaScript in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-13696	N/A	A-GOO-CHRO- 031219/47
Use After Free	25-11-2019	6.8	Use after free in media in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted	N/A	A-GOO-CHRO- 031219/48

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			HTML page.		
			CVE ID : CVE-2019-13699		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-11-2019	6.8	Out of bounds memory access in the gamepad API in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-13700	N/A	A-G00-CHR0- 031219/49
Authenticati on Bypass by Spoofing	25-11-2019	4.3	Incorrect implementation in navigation in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  CVE ID: CVE-2019-13701	N/A	A-G00-CHR0- 031219/50
Improper Privilege Management	25-11-2019	6.8	Inappropriate implementation in installer in Google Chrome on Windows prior to 78.0.3904.70 allowed a local attacker to perform privilege escalation via a crafted executable.  CVE ID: CVE-2019-13702	N/A	A-G00-CHR0- 031219/51
Authenticati on Bypass by Spoofing	25-11-2019	4.3	Insufficient policy enforcement in the Omnibox in Google Chrome on Android prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	N/A	A-GOO-CHRO- 031219/52

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID		
			CVE I	D : CVE-	2019-1	3703						
Authenticati on Bypass by Spoofing	25-11-2019	4.3	enfor Goog 78.0.3 remo conte crafte	ficient po cement i le Chrom 3904.70 te attack ent secur ed HTML	n navigate prior allowed er to by ity polic page.	to a pass y via a	N/A		A-G00-0 031219			
			Insuf	ficient po	olicy							
Information Exposure	25-11-2019	4.3	Googl 78.0.3 attacl user t exten origin	cement i le Chrom 3904.70 ker who to install sion to le n data via me Exter	ne prior allowed convince a malici eak cros	to an ed a ous s-	N/A		A-G00-0 031219			
			CVE I	D : CVE-	2019-1	3705						
Out-of- bounds Read	25-11-2019	6.8	Out of bounds memory access in PDFium in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.  CVE ID: CVE-2019-13706				N/A		A-G00-0 031219			
Information Exposure	25-11-2019	4.3	Insufficient validation of untrusted input in intents in Google Chrome on Android prior to 78.0.3904.70 allowed a local attacker to leak files via a crafted application.  CVE ID: CVE-2019-13707				N/A		A-G00-CHR0 031219/56			
Authenticati on Bypass by	25-11-2019	4.3	Inappropriate implementation in						N/A		A-G00-CHR0- 031219/57	
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3	<b>2-3</b> 3-4 4-5 5-6			6-7	7-8	8-9	9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Spoofing			navigation in Google Chrome on iOS prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.  CVE ID: CVE-2019-13708		
Authenticati on Bypass by Spoofing	25-11-2019	4.3	Insufficient policy enforcement in downloads in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass download restrictions via a crafted HTML page.	N/A	A-G00-CHR0- 031219/58
			CVE ID : CVE-2019-13709		
Improper Input Validation	25-11-2019	4.3	Insufficient validation of untrusted input in downloads in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass download restrictions via a crafted HTML page.	N/A	A-G00-CHR0- 031219/59
Information Exposure	25-11-2019	5	Insufficient policy enforcement in JavaScript in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to leak cross-origin data via a crafted HTML page.  CVE ID: CVE-2019-13711	N/A	A-G00-CHR0- 031219/60
Information Exposure	25-11-2019	4.3	Insufficient policy enforcement in JavaScript in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to leak cross-origin data via a	N/A	A-GOO-CHRO- 031219/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patc	h	NCIIPO	CID
			crafted HTML page.				
			CVE ID: CVE-2019-13713				
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	25-11-2019	4.3	Insufficient validation of untrusted input in Color Enhancer extension in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to inject CSS into an HTML page via a crafted URL.  CVE ID: CVE-2019-13714	N/A		A-G00-0 031219/	
Authenticati on Bypass by Spoofing	25-11-2019	4.3	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.  CVE ID: CVE-2019-13715	N/A		A-G00-0 031219/	
Insecure Storage of Sensitive Information	25-11-2019	4.3	Incorrect security UI in full screen mode in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to hide security UI via a crafted HTML page.  CVE ID: CVE-2019-13717	N/A		A-G00-0 031219/	
Improper Input Validation	25-11-2019	4.3	Insufficient data validation in Omnibox in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.  CVE ID: CVE-2019-13718	N/A		A-G00-0 031219/	
Insecure	25-11-2019	4.3	Incorrect security UI in full	N/A		A-G00-0	HRO-
CV Scoring Scal (CVSS)	le 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Storage of Sensitive Information			screen mode in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to hide security UI via a crafted HTML page.  CVE ID: CVE-2019-13719		031219/66
Use After Free	25-11-2019	6.8	Use after free in WebAudio in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	N/A	A-G00-CHR0- 031219/67
Use After Free	25-11-2019	6.8	Use after free in PDFium in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-13721	N/A	A-G00-CHR0- 031219/68
Use After Free	25-11-2019	4.3	Use after free in Blink in Google Chrome prior to 75.0.3770.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-5842	N/A	A-G00-CHR0- 031219/69
Use After Free	25-11-2019	6.8	Use after free in offline mode in Google Chrome prior to 76.0.3809.87 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape	N/A	A-GOO-CHRO- 031219/70

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page.		
			CVE ID: CVE-2019-5850		
Use After Free	25-11-2019	6.8	Use after free in WebAudio in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.  CVE ID: CVE-2019-5851	N/A	A-GOO-CHRO- 031219/71
IBM					
security_iden	tity_manager				
Deserializati on of Untrusted Data	20-11-2019	9.3	IBM Security Identity Manager 6.0.0 could allow a remote attacker to execute arbitrary code on the system, caused by the deserialization of untrusted data. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 166456.  CVE ID: CVE-2019-4561	https://ww w.ibm.com/ support/pa ges/node/1 108695	A-IBM-SECU- 031219/72
maximo_asse	t_managemen	it			
Improper Authenticati on	20-11-2019	5.5	IBM Maximo Asset Management 7.6, 7.6.1, and 7.6.1.1 could allow an authenticated user to delete a record that they should not normally be able to. IBM X- Force ID: 165586.  CVE ID: CVE-2019-4530	https://ww w.ibm.com/ support/pa ges/node/1 108503	A-IBM-MAXI- 031219/73
smartcloud_a	nalytics_log_a	nalysi	5		
Incorrect	22-11-2019	4.3	IBM SmartCloud Analytics	https://ww	A-IBM-SMAR-
CV Scoring Scal (CVSS)	le 0-1	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	:ch	NCIIP	C ID
Authorizatio n			set the author session allow sensite man in technic 15918	through e secure rization on cookie an attac rive infor n the mid iques. IB B5. D: CVE-	attribut tokens o es. This o ker to o mation ddle M X-For	te on or could btain using rce ID:	w.ibm suppo ges/no 11017	rt/pa ode/1	031219	/74
Improper Input Validation	22-11-2019	4.3	1.3.1 the victim Web so could vulne victim possill attack	through a remote the click the click tim. By to visit exploit t rability t oly launc as agains f-Force II	1.3.5 co e attack king act persuad a malici mote att this to hijack actions a ch furthe t the vice D: 1591	uld er to ion of ding a ous cacker the and er etim. 86.	https:/ w.ibm suppo ges/no 10976	.com/ rt/pa ode/1	A-IBM-S 031219	
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	22-11-2019	4.9	1.3.1 to vulne heade could poison IBM X	martClo through rable to rable to lead to I ning or f (-Force II	1.3.5 is possible on attac HTTP ca irewall l D: 1591	e host k that che bypass. 87.	https:/ w.ibm suppo ges/no 10974	.com/ rt/pa ode/1	A-IBM-S 031219	
Information Exposure	22-11-2019	3.6	1.3.1 tunaut inforr solrco allow	martClo through horized nation li onfig.xml an attac otive adr	1.3.5 all disclost ke acces and cou ker to p	ows are of ssing ald erform	https:/ w.ibm suppo ges/no 10972	.com/ rt/pa ode/1	A-IBM-S 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID		
			tasks. 15952		Force ID	:						
					2019-4	243						
infoway			CVLI	D.CVL	2017 1	213						
social_photo_	gallery											
Social_photo_	Builtiy		The S	ocial Pho	oto Galle	erv						
Improper Input Validation	18-11-2019	4.6	plugin 1.0 for WordPress allows Remote Code Execution by creating an album and attaching a		N/A		A-INF-S 031219					
iobroker												
iobroker.adm	iin											
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-11-2019	7.5	3.6.12 include outside direct	iobroker.admin before 3.6.12 allows attacker to include file contents from outside the `/log/file1/` directory.  CVE ID: CVE-2019-10765		N/A		A-IOB-I 031219	_			
iterm2												
iterm2												
Information Exposure	17-11-2019	5	iTerm2 through 3.3.6 has potentially insufficient documentation about the presence of search history in com.googlecode.iterm2.plist, which might allow remote attackers to obtain sensitive information, as demonstrated by searching for the NoSyncSearchHistory string in .plist files within		documentation about the bresence of search history in com.googlecode.iterm2.plist, which might allow remote attackers to obtain sensitive information, as demonstrated by searching for the NoSyncSearchHistory		cially insufficient nentation about the nece of search history in coglecode.iterm2.plist, might allow remote ners to obtain sensitive nation, as nstrated by searching NoSyncSearchHistory		N/A		A-ITE-I' 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3			6-7	7-8	8-9	9-10			

Weakness	Publish Date	cvss	Descripti	on & CVE	ID	Pat	:ch	NCIIP	C ID
			public Git rep						
			CVE ID : CVE	-2019-19	9022				
Jenkins									
support_core								1	
Improper Preservation of Permissions	21-11-2019	5.5	A missing per in Jenkins Sup Plugin 2.63 an allows attack Overall/Read delete support CVE ID: CVE	oport Connd earlieners with permissert bundle	re r ion to s.	https:/kins.io rity/ac y/201 21/#S ITY-16	/secu dvisor 9-11- ECUR	A-JEN-S 031219	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-11-2019	5.5	A path traver vulnerability Support Core and earlier al with Overall/permission to arbitrary files master.  CVE ID : CVE	https:/kins.io rity/ac y/201 21/#S ITY-16	/secu dvisor 9-11- ECUR	A-JEN-S 031219			
google_comp	ute_engine								
Authorizatio n Bypass Through User- Controlled Key	21-11-2019	4.3	Engine Plugir earlier does n host keys who agents create enabling man attacks.	earlier does not verify SSH host keys when connecting agents created by the plugin, enabling man-in-the-middle 2		https:/kins.io rity/ac y/201 21/#S ITY-15	/secu dvisor 9-11- ECUR	A-JEN-G 031219	
Incorrect Permission Assignment for Critical Resource	21-11-2019	4	in various AP Jenkins Googl Engine Plugir earlier allow Overall/Read				/secu dvisor 9-11- ECUR	A-JEN-G 031219	
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish	Date	cvss		Description	on & CVE	ID	Pat	ch:	NCIIP	CID			
				envir	onment.									
				CVE I	D : CVE-	2019-1	6547							
Cross-Site Request Forgery (CSRF)	21-11-	2019	6.8	vulne Googl Plugir Comp ovisio provis	Vulnerability in Jenkins Google Compute Engine Plugin 4.1.1 and earlier in ComputeEngineCloud#doPr ovision could be used to provision new agents.			A cross-site request forgery vulnerability in Jenkins Google Compute Engine Plugin 4.1.1 and earlier in ComputeEngineCloud#doPr ovision could be used to provision new agents.  CVE ID: CVE-2019-16548		lity in Jenkins mpute Engine .1 and earlier in EngineCloud#doPr uld be used to new agents.		//jen /secu dvisor 9-11- ECUR 586	A-JEN-G 031219	
jhead_project														
jhead	jhead													
Out-of- bounds Read	17-11-	2019	4.3	heap- The in service ReadJ proce The a specia	jhead 3.03 is affected by: heap-based buffer over-read. The impact is: Denial of service. The component is: ReadJpegSections and process_SOFn in jpgfile.c. The attack vector is: Open a specially crafted JPEG file.  CVE ID: CVE-2019-19035			N/A		A-JHE-JI 031219				
kairosdb_pro	ject													
kairosdb														
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-11-	2019	4.3	xss ir show js/gra by vie '"sam >' sub	KairosDB through 1.2.2 has XSS in view.html because of showErrorMessage in js/graph.js, as demonstrated by view.html?q= with a ""sampling":{"value":" <script>' substring.  CVE ID: CVE-2019-19040</td><td>N/A</td><td></td><td>A-KAI-K 031219</td><td></td></tr><tr><td>Lenovo</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>customer_eng</td><td>gagemei</td><td>nt_ser</td><td>vice</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Improper Privilege Management</td><td>20-11-</td><td>2019</td><td>4.6</td><td colspan=3>A potential vulnerability in the discontinued Customer Engagement Service (CCSDK) software version</td><td colspan=2>e discontinued Customer ngagement Service</td><td></td><td colspan=2>A-LEN-CUST- 031219/88</td></tr><tr><td>CV Scoring Scal (CVSS)</td><td>e 0-</td><td>-1</td><td>1-2</td><td>2-3</td><td colspan=3></td><td>6-7</td><td>7-8</td><td>8-9</td><td>9-10</td></tr></tbody></table></script>									

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			2.0.21.1 may allow local privilege escalation.		
			CVE ID : CVE-2019-6184		
system_interf	ace_foundation	on			
N/A	20-11-2019	6.5	A potential vulnerability was reported in Lenovo System Interface Foundation versions before v1.1.18.3 that could allow an authenticated user to execute code as another user.  CVE ID: CVE-2019-6186	N/A	A-LEN-SYST- 031219/89
Untrusted Search Path	20-11-2019	4.4	A potential vulnerability was reported in Lenovo System Interface Foundation versions before v1.1.18.3 that could allow an administrative user to load an unsigned DLL.  CVE ID: CVE-2019-6189	N/A	A-LEN-SYST- 031219/90
xclarity_contr	oller				
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.	N/A	A-LEN-XCLA- 031219/91

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Pub	lish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
				CVE I	D : CVE-	2019-6	187				
paper											
Improper Privilege Management	20-1	11-2019	4.6	the di Lenov versional	A potential vulnerability in the discontinued LenovoPaper software version 1.0.0.22 may allow local privilege escalation.  CVE ID: CVE-2019-6191					A-LEN-I 031219	
limnoria_proj	ject										
limnoria											
Improper Input Validation	16-2	11-2019	7.5	pluging 2019. (through allow attack informunspecting the case communication)	Eval injection in the Math plugin of Limnoria (before 2019.11.09) and Supybot (through 2018-05-09) allows remote unprivileged attackers to disclose information or possibly have unspecified other impact via the calc and icalc IRC commands.  CVE ID: CVE-2019-19010					A-LIM-L 031219	
Microfocus											
operations_ag	gent										
Improper Restriction of XML External Entity Reference ('XXE')	18-2	11-2019	4	Micro Agent 12.01 12.05 The v explo on Op	XXE attack vulnerability on Micro Focus Operations Agent, affected version 12.0, 12.01, 12.02, 12.03, 12.04, 12.05, 12.06, 12.10, 12.11. The vulnerability could be exploited to do an XXE attack on Operations Agent.  CVE ID: CVE-2019-17085			https://soft waresuppor t.softwaregr p.com/doc/ KM035564 26		A-MIC-0 031219	
Netapp											
ontap_select_	deplo	oy_admi	nistrat	ion_uti	lity						
Improper Neutralizatio n of Special		11-2019	7.5	admii	administration utility urit			https://urity.n	etap	A-NET-0 031219	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	l	Description	on & CVE	ID	Pat	ch	NCIIP	CID
Elements in Output Used by a Downstream Component ('Injection')			code i which explo unaut attack privil	are sus njection when s ited could henticate to en eged use D: CVE-	vulnera uccessfu ld allow ted remo able and er accour	ability ally an ote I use a nt.	sory/r 20191 0001/	121-		
Improper Input Validation	21-11-2019	6.5	Deplo are su vulne succe allow to esc	rsions o y admin asceptibl rability v ssfully e an admi alate the <b>D : CVE-</b>	istration e to a which w xploited inistration	hen could ve user eges.	https:/ urity.n p.com/ sory/r 20191 0002/	etap /advi itap- 121-	A-NET-0 031219	
ngiflib_projec	:t									
ngiflib										
NULL Pointer Dereference	17-11-2019	5	NULL GifInd ngiflil palett	PnP ngi pointer lexToTr o.c via a e.  D: CVE-	derefer ueColor file that	ence in in lacks a	N/A		A-NGI-N 031219	
Nvidia										
gpumodeswit	ch									
Improper Privilege Management	18-11-2019	7.2	Tool p GPUM to 202 mode nvflsh nvflsh vulne authe admin gain a	NVIDIA NVFlash, NVUFlash Tool prior to v5.588.0 and GPUModeSwitch Tool prior to 2019-11, NVIDIA kernel mode driver (nvflash.sys, nvflsh32.sys, and nvflsh64.sys) contains a vulnerability in which authenticated users with administrative privileges can gain access to device memory and registers of					A-NVI-0 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			by NV to esc inform denia	devices 'IDIA, wlation of the control of the contro	nich may of privile isclosur ice.	y lead eges, e, or				
nvflash			CVET	DIGVE	2017 0					
Improper Privilege Management	18-11-2019	7.2	Tool p GPUM to 202 mode nvflsh nvflsh vulne admin gain a memo other by NV to esc information	NVIDIA NVFlash, NVUFlash Tool prior to v5.588.0 and GPUModeSwitch Tool prior to 2019-11, NVIDIA kernel mode driver (nvflash.sys, nvflsh32.sys, and nvflsh64.sys) contains a vulnerability in which authenticated users with administrative privileges can gain access to device memory and registers of other devices not managed by NVIDIA, which may lead to escalation of privileges, information disclosure, or denial of service.  CVE ID: CVE-2019-5688			N/A		A-NVI-1 031219	
nvuflash										
Improper Privilege Management	18-11-2019	7.2	NVIDIA NVFlash, NVUFlash Tool prior to v5.588.0 and GPUModeSwitch Tool prior to 2019-11, NVIDIA kernel mode driver (nvflash.sys, nvflsh32.sys, and nvflsh64.sys) contains a vulnerability in which authenticated users with administrative privileges can gain access to device memory and registers of other devices not managed				N/A		A-NVI-1 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID				Pat	ch	NCIIF	PC ID
			by NVIDIA, which may lead to escalation of privileges, information disclosure, or denial of service.							
			CVE II	D : CVE-	2019-5	688				
octopus										
server										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-11-2019	3.5	scripti in Octo throug remot attack web so	sistent cross-site ting (XSS) vulnerability topus Server 3.4.0 ugh 2019.10.5 allows te authenticated kers to inject arbitrary script or HTML. UD: CVE-2019-19085			A-0CT- 031219			
octopus_depl	ov		GVE	3. GVE	2017 1	7005				
Unrestricted Upload of File with Dangerous Type	18-11-2019	4	throug auther Packag upload upload packag except under	In Octopus Deploy 3.3.0 through 2019.10.4, an authenticated user with PackagePush permission to upload packages could upload a maliciously crafted package, triggering an exception that exposes underlying operating system details.					A-OCT- 031219	
oniguruma_p	roject									
oniguruma										
Integer Overflow or Wraparound	17-11-2019	7.5	An integer overflow in the search_in_range function in regexec.c in Oniguruma 6.x before 6.9.4_rc2 leads to an out-of-bounds read, in which the offset of this read is under the control of an attacker. (This only affects the 32-bit compiled version).				N/A		A-ONI-0 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			a deni inforn possil other	te attack ial-of-se mation d oly have impact, ar expre	rvice or isclosur unspeci via a cra	e, or fied				
			CVE I	D : CVE-	2019-1	9012				
openfind										
mail2000										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-11-2019	4.3	MAIL: 6.0 an script allow: arbitr paran authe execu access vulne mail s organ and u	/cgi-bin, 2000 thing (XSS) ing executary code neter with ted for a sing the rability a system of izations niversiti D: CVE-	rough vest a cross of vulner ution of evia ACT thout on The country user page. The affects markets of governation, companies.	ersion s-site rability,  FION ode can nis nany nments, nies	https://github/chtse y/211 93640 d010a bee21 https://github/tonyl/9563 e0c836 bd3db 84e27 https://twcert w/taiv/TVN- 20190 https://w.opencom.tv	com curit 19b3 bea1 b9e3 6d, //gist. .com kuo76 8395 e68d 0fa01 ,/tvn. corg.t vanvn 9001, //ww nfind. v/tai esour	A-OPE-1 031219	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	20-11-2019	4.3	bin/p throughas a (XSS) execu	ogin feat ortal" in gh versic cross-sit vulnera tion of a	MAIL2( on 6.0 ance script bility, al rbitrary	000 nd 7.0 ing lowing code	https:/ github /chtse y/b33 0d468 7fb266 7ef24a	.com curit 9650 6ad4	A-OPE-1 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	l	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Scripting')			mail s organ and u	rability a system o izations niversiti <b>D : CVE</b> -	f goverr . compa es.	nments, nies	https:/github /tonyk /5bf1a d953d afe0a2 2147, https:/ twcert w/taiv /TVN- 20190 https:/ w.oper com.tv wan/r ce.htm	.com kuo76 hc369 5276 d04c //tvn. .org.t vanvn 9002, //ww nfind. v/tai esour		
URL Redirection to Untrusted Site ('Open Redirect')	20-11-2019	5.8	An Open Redirect vulnerability for all browsers in MAIL2000 through version 6.0 and 7.0, which will redirect to a malicious site without authentication. This vulnerability affects many mail system of governments, organizations, companies and universities.  CVE ID: CVE-2019-15073				https://github/chtse y/512 24ddd 21cf5f 6f90f, https://github/tonyk/ed1cc 755bft 7ca24f ed13, https://twcert w/taiv/TVN- 20190 https://w.open com.tv wan/r ce.htm	com curit ebad ffb53 1a33 //gist. .com kuo76 c21cf b8b6 f50bd //tvn. .org.t vanvn 9003, //ww nfind. v/tai esour	A-OPE-1 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIPC ID
openwrt						
openwrt						
Improper Certificate Validation	18-11-2019	4.3	An exploitable information leak vulnerability exists in the ustream-ssl library of OpenWrt, versions 18.06.4 and 15.05.1. When connecting to a remote server, the server's SSL certificate is checked but no action is taken when the certificate is invalid. An attacker could exploit this behavior by performing a man-in-the-middle attack, providing any certificate, leading to the theft of all the data sent by the client during the first request. After an SSL connection is initialized via _ustream_ssl_init, and after any data (e.g. the client's HTTP request) is written to the stream using ustream_printf, the code eventually enters the function _ustream_ssl_poll, which is used to dispatch the read/write events  CVE ID: CVE-2019-5101	N/A		A-OPE-OPEN- 031219/107
Improper Certificate Validation	18-11-2019	4.3	An exploitable information leak vulnerability exists in the ustream-ssl library of OpenWrt, versions 18.06.4 and 15.05.1. When connecting to a remote server, the server's SSL certificate is checked but no action is taken when the	N/A		A-OPE-OPEN- 031219/108
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			certificate is invalid. An attacker could exploit this behavior by performing a man-in-the-middle attack, providing any certificate, leading to the theft of all the data sent by the client during the first request.		
Pimcore			CVE ID : CVE-2019-5102		
pimcore					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	18-11-2019	4	pimcore/pimcore before 6.3.0 is vulnerable to SQL Injection. An attacker with limited privileges (classes permission) can achieve a SQL injection that can lead in data leakage. The vulnerability can be exploited via 'id', 'storeId', 'pageSize' and 'tables' parameters, using a payload for trigger a time based or error based sql injection.  CVE ID: CVE-2019-10763	N/A	A-PIM-PIMC- 031219/109
pixie_project					
pixie					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	19-11-2019	7.5	Pixie versions 1.0.x before 1.0.3, and 2.0.x before 2.0.2 allow SQL Injection in the limit() function due to improper sanitization.  CVE ID: CVE-2019-10766	N/A	A-PIX-PIXI- 031219/110
Postgresql					
postgresql-co	mmon				
CV Scoring Scal (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Improper Privilege Management	20-11-2019	7.2	postg version drop creati tempo which	g_ctlclus resql-co ons prion privilege ng socke orary din o could r ege esca	mmon in to 210 es when et/statis rectories esult in	didn't tics	N/A		A-POS-I 031219	
			CVE I	D : CVE-	2019-3	466				
qmetry										
jenkins_qmet	ry_for_jira									
Insufficiently Protected Credentials	21-11-2019	4	Test M 1.12 a crede job co Jenkin can be Exten or acc systen	D : CVE-	nent Plu er store nencrypt files on r where l by user d permi ne maste	gin s ted in the they s with ssion, or file	https:/ kins.io rity/ac y/201 21/#S ITY- 727%2	/secu lvisor 9-11- ECUR	A-QME- 031219	•
Insufficiently Protected Credentials	21-11-2019	4	Test Netransic configuration forms in the	ns QMeta Managen mits crea guration of job con s, potent ir expos D: CVE-	nent Plu dentials in plain nfigurati ially resi ure.	gin in its text as on ulting	https:/ kins.io rity/ac y/201 21/#S ITY- 727%2	/secu lvisor 9-11- ECUR	A-QME- 031219	
Qualcomm										
ips										
Integer Overflow or Wraparound	21-11-2019	7.5	overfi PostS code t	teger overflow to buffer erflow vulnerability in stScript image handling de used by the PostScript- d PDF-compatible terpreters due to incorrect		bility in w.qualcom handling m.com/com PostScript- pany/prod ible ct-		com /com orodu	A-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	6-7 7-8		9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			buffer size calculation. in PostScript and PDF printers that use IPS versions prior to 2019.2 in PostScript and PDF printers that use IPS versions prior to 2019.2				lletins ber-20 bulleti	19-		
C.			CVE I	D : CVE-	2019-1	0627				
rconfig										
rconfig	<u> </u>		1				T			
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	21-11-2019	6.5	device SQL in	njection.	earchCo		N/A		A-RCO-I 031219	
Redhat										
jboss_fuse										
Improper Restriction of XML External Entity Reference ('XXE')	18-11-2019	5	org.co n-map XML e vulne 2016- codeh asl lib	A flaw was found in org.codehaus.jackson:jackson-mapper-asl:1.9.x libraries. XML external entity vulnerabilities similar CVE-2016-3720 also affects codehaus jackson-mapper-asl libraries but in different classes.			https:/ zilla.re com/s bug.cg CVE-2 10172	edhat. how_ i?id= 019-	A-RED-J 031219	
jboss_enterpr	rise annlicati	on plat								
Improper Restriction of XML External Entity Reference ('XXE')	18-11-2019	5	A flaw was found in org.codehaus.jackson:jackson-mapper-asl:1.9.x libraries. XML external entity vulnerabilities similar CVE-2016-3720 also affects codehaus jackson-mapper-				https:/ zilla.re com/s bug.cg CVE-2 10172	edhat. how_ i?id= 019-	A-RED-J 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			asl libraries but in different classes.		
D I '			CVE ID : CVE-2019-10172		
Redmine					
redmine					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	21-11-2019	4	A SQL injection vulnerability in Redmine through 3.2.9 and 3.3.x before 3.3.10 allows Redmine users to access protected information via a crafted object query.  CVE ID: CVE-2019-18890	N/A	A-RED-REDM- 031219/118
sandline					
centraleyezer	[				
Unrestricted Upload of File with Dangerous Type	18-11-2019	7.5	Sandline Centraleyezer (On Premises) allows unrestricted File Upload with a dangerous type, because the feature of adding ".jpg" to any uploaded filename is not enforced on the server side.  CVE ID: CVE-2019-12271	N/A	A-SAN-CENT- 031219/119
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-11-2019	4.3	Sandline Centraleyezer (On Premises) allows Stored XSS using HTML entities in the name field of the Category section.  CVE ID: CVE-2019-12299	N/A	A-SAN-CENT- 031219/120
Improper Neutralizatio n of Input During Web Page	18-11-2019	4.3	Sandline Centraleyezer (On Premises) allows Unrestricted File Upload leading to Stored XSS. An HTML page running a script	N/A	A-SAN-CENT- 031219/121
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	-8 8-9 9-10

Generation ('Cross-site Scripting')  simplito elliptic-php  Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')  Symantec norton_app_lock	-11-2019	5.8	could be uploaded to the server. When a victim tries to download a CISO Report template, the script is loaded.  CVE ID: CVE-2019-12311  In elliptic-php versions priot to 1.0.6, Timing attacks might be possible which can result in practical recovery of the long-term private key generated by the library under certain conditions.  Leakage of a bit-length of the scalar during scalar	N/A	A-SIM-ELLI-
Concurrent Execution using Shared Resource with 18- Improper Synchronizat ion ('Race Condition')	-11-2019	5.8	to 1.0.6, Timing attacks might be possible which can result in practical recovery of the long-term private key generated by the library under certain conditions. Leakage of a bit-length of the	N/A	A-SIM-ELLI-
Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')  Symantec	-11-2019	5.8	to 1.0.6, Timing attacks might be possible which can result in practical recovery of the long-term private key generated by the library under certain conditions. Leakage of a bit-length of the	N/A	A-SIM-ELLI-
			multiplication is possible on an elliptic curve which might allow practical recovery of the long-term private key.  CVE ID: CVE-2019-10764		031219/122
- • • -					
N/A 18-	-11-2019	4.4	Norton App Lock, prior to 1.4.0.503, may be susceptible to a bypass exploit. In this type of circumstance, the exploit can allow the user to circumvent the app to prevent it from locking other apps on the device, thereby allowing the individual to gain access.  CVE ID: CVE-2019-18373	https://sup port.symant ec.com/us/ en/article.S YMSA1496. html	A-SYM-NORT- 031219/123
Vmware					
workstation					

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	20-11-2019	4	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an information disclosure vulnerability in vmnetdhcp. Successful exploitation of this issue may allow an attacker on a guest VM to disclose sensitive information by leaking memory from the host process.  CVE ID: CVE-2019-5540	https://ww w.vmware.c om/securit y/advisorie s/VMSA- 2019- 0021.html	A-VMW- WORK- 031219/124
Out-of- bounds Write	20-11-2019	6.5	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an out-of-bounds write vulnerability in the e1000e virtual network adapter. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition on their own VM.  CVE ID: CVE-2019-5541	https://ww w.vmware.c om/securit y/advisorie s/VMSA- 2019- 0021.html	A-VMW- WORK- 031219/125
Improper Input Validation	20-11-2019	4	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain a denial-of-service vulnerability in the RPC handler. Successful exploitation of this issue may allow attackers with normal user privileges to create a denial-of-service condition on their own VM.  CVE ID: CVE-2019-5542	https://ww w.vmware.c om/securit y/advisorie s/VMSA- 2019- 0021.html	A-VMW- WORK- 031219/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fusion			L		
Information Exposure	20-11-2019   4		VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an information disclosure vulnerability in vmnetdhcp. Successful exploitation of this issue may allow an attacker on a guest VM to disclose sensitive information by leaking memory from the host process.  CVE ID: CVE-2019-5540	https://ww w.vmware.c om/securit y/advisorie s/VMSA- 2019- 0021.html	A-VMW-FUSI- 031219/127
Out-of- bounds Write	20-11-2019	6.5	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an out-of-bounds write vulnerability in the e1000e virtual network adapter. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition on their own VM.  CVE ID: CVE-2019-5541	https://ww w.vmware.c om/securit y/advisorie s/VMSA- 2019- 0021.html	A-VMW-FUSI- 031219/128
Improper Input Validation	20-11-2019	4	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain a denial-of-service vulnerability in the RPC handler. Successful exploitation of this issue may allow attackers with normal user privileges to create a denial-of-service condition on their own VM.	https://ww w.vmware.c om/securit y/advisorie s/VMSA- 2019- 0021.html	A-VMW-FUSI- 031219/129

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			CVE I	D : CVE-	2019-5	542				
xorur										
lpar2rrd										
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	17-11-2019	9	An issue was discovered in Xorux Lpar2RRD 6.11 and Stor2RRD 2.61, as distributed in Xorux 2.41. They do not correctly verify the integrity of an upgrade package before processing it. As a result, official upgrade packages can be modified to inject an arbitrary Bash script that will be executed by the underlying system. It is possible to achieve this by modifying the values in the files.SUM file (which are used for integrity control) and injecting malicious code into the upgrade.sh file.  CVE ID: CVE-2019-19041				N/A		A-XOR- 031219	
stor2rrd										
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	17-11-2019	9	An issue was discovered in Xorux Lpar2RRD 6.11 and Stor2RRD 2.61, as distributed in Xorux 2.41. They do not correctly verify the integrity of an upgrade package before processing it. As a result, official upgrade packages can be modified to inject an arbitrary Bash script that will be executed by the underlying system. It is possible to achieve this by modifying the values in the files.SUM file (which are used for integrity control)				N/A		A-XOR-: 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID		Patch	NCIIPC ID
			and injecting malicious into the upgrade.sh file.			
			CVE ID : CVE-2019-190			
			CVE ID : CVE-2019-190	741		
xorur					T	
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	17-11-2019	9	An issue was discovered in Xorux Lpar2RRD 6.11 and Stor2RRD 2.61, as distributed in Xorux 2.41. They do not correctly verify the integrity of an upgrade package before processing it. As a result, official upgrade packages can be modified to inject an arbitrary Bash script that will be executed by the underlying system. It is possible to achieve this by modifying the values in the files.SUM file (which are used for integrity control) and injecting malicious code into the upgrade.sh file.  CVE ID: CVE-2019-19041			A-XOR-XORU- 031219/132
			Operating System			
Apple						
mac_os_x						
Information Exposure	20-11-2019	4	VMware Workstation (1 before 15.5.1) and Fusio (11.x before 11.5.1) con an information disclosu vulnerability in vmnetd Successful exploitation of this issue may allow an attacker on a guest VM to disclose sensitive information by leaking memory from the host process.	tain http w.vr om/ y/ac s/Vi 2014	s://ww nware.c securit lvisorie MSA- 9- 1.html	O-APP-MAC 031219/133
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9 9-10

Weakness	Pul	blish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
				CVE I	CVE ID : CVE-2019-5540						
Out-of- bounds Write	20-	11-2019	6.5	befor (11.x an ou vulne virtua Succe this is executhe guattack of-ser own V	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an out-of-bounds write vulnerability in the e1000e virtual network adapter. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition on their own VM.  CVE ID: CVE-2019-5541				//ww vare.c curit sorie sA-	O-APP-1 031219	_
Canonical											
ubuntu_linux											
Improper Privilege Management	20-	11-2019	7.2	postg version drop creati tempo which	The pg_ctlcluster script in postgresql-common in versions prior to 210 didn't drop privileges when creating socket/statistics temporary directories, which could result in local privilege escalation.			N/A		0-CAN- 031219	
Debian											
debian_linux											
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	21-	11-2019	4	in Recand 3 allow acces	A SQL injection vulnerability in Redmine through 3.2.9 and 3.3.x before 3.3.10 allows Redmine users to access protected information via a crafted object query.  CVE ID: CVE-2019-18890			N/A		O-DEB-1 031219	
Improper	20-	11-2019	7.2	The pg_ctlcluster script in				N/A		O-DEB-	DEBI-
CV Scoring Scal (CVSS)	е	0-1	1-2	2-3					7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			postgresql-common in versions prior to 210 didn't drop privileges when creating socket/statistics temporary directories, which could result in local privilege escalation.  CVE ID: CVE-2019-3466		031219/137
Fedoraprojec	:t				
fedora					
Improper Input Validation	16-11-2019	7.5	Eval injection in the Math plugin of Limnoria (before 2019.11.09) and Supybot (through 2018-05-09) allows remote unprivileged attackers to disclose information or possibly have unspecified other impact via the calc and icalc IRC commands.  CVE ID: CVE-2019-19010	N/A	O-FED-FEDO- 031219/138
Fortinet					
fortios					
Use of Hard- coded Credentials	21-11-2019	4	Use of a hard-coded cryptographic key to cipher sensitive data in FortiOS configuration backup file may allow an attacker with access to the backup file to decipher the sensitive data, via knowledge of the hard-coded key. The aforementioned sensitive data includes users' passwords (except the administrator's password), private keys' passphrases and High Availability	https://fort iguard.com /advisory/F G-IR-19- 007	O-FOR-FORT- 031219/139

CV Scoring Scale	0-1	1_2	2-3	3-/1	4-5	5-6	6-7	7-8	8-0	9-10
(CVSS)	0	1-2	2-3	7	4-5	3	0-7	7-8	0	J-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			passv	vord (wh	en set).					
			CVE I	D : CVE-	2019-6	693				
Lenovo							•			
thinkpad_usb-c_dock_firmware										
N/A	20-11-2019	5	repor Dock may a service	ential vu ted in Th Firmwan illow a d ce. <b>D : CVE</b> -	ninkPad re versic enial of	USB-C on 3.7.2	N/A		O-LEN-7 031219	
Linksys										
velop_whw03	03_firmware									
Authorizatio n Bypass Through User- Controlled Key	21-11-2019	6.4	1.1.8. remo the re reque /sysin	n Linksys 192419 te attack ecovery kest for the nfo_json. <b>D: CVE-</b>	devices ers to di xey via a e cgi URI.	iscover direct	N/A		O-LIN-V 031219	
velop_whw03	 									
Authorizatio n Bypass Through User- Controlled Key	21-11-2019	6.4	1.1.8. remo the re reque /sysin	n Linksys 192419 ( te attack ecovery k est for the nfo_json. <b>D : CVE-</b>	devices ers to di xey via a e cgi URI.	scover direct	N/A		O-LIN-V 031219	
velop_whw03	01_firmware									
Authorizatio n Bypass Through User- Controlled Key	21-11-2019	6.4	Belkin Linksys Velop 1.1.8.192419 devices allows remote attackers to discover the recovery key via a direct request for the /sysinfo_json.cgi URI.  CVE ID: CVE-2019-16340				N/A		O-LIN-V 031219	
Linux										
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID				Pat	ch	NCIIF	PC ID
linux_kernel		ı								
Unrestricted Upload of File with Dangerous Type	18-11-2019	7.5	of Apainsect ENAB S confidence on the section of th	.1.1 and ache Solute setting LE_REM figuration by the solution of the solution	containing for the OTE_JM on option ash file ship ou use the ship of the ship of the ship of the ship of the ship opened for exercise to you appear to anyone as to you appear to a for exercise to ex	n an he X_OPT h in the oping he rom then he on 8983), cation. For r with hr Solr hccess n	N/A		0-LIN-I 031219	
NULL Pointer Dereference	21-11-2019	4.3	btrfs_root_node in fs/btrfs/ctree.c in the Linux kernel through 5.3.12 allows a NULL pointer dereference because rcu_dereference(root- >node) can be zero.  CVE ID: CVE-2019-19036  ext4_empty_dir in				N/A		0-LIN-I 031219	
NULL Pointer Dereference	21-11-2019	4.3	kerne a NUL becau ext4_1	:4/name l through L pointe se read_dirl	h 5.3.12 er derefe olock(in	allows erence ode,0,	N/A		O-LIN-I 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			zero.  CVE ID : CVE-2019-19037		
Information Exposure	21-11-2019	1.9	btrfs_free_extent in fs/btrfs/extent-tree.c in the Linux kernel through 5.3.12 calls btrfs_print_leaf in a certain ENOENT case, which allows local users to obtain potentially sensitive information about register values via the dmesg program.  CVE ID: CVE-2019-19039	N/A	O-LIN-LINU- 031219/147
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the i40e_setup_macvlans() function in drivers/net/ethernet/intel/i 40e/i40e_main.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering i40e_setup_channel() failures, aka CID-27d461333459.  CVE ID: CVE-2019-19043	N/A	O-LIN-LINU- 031219/148
Uncontrolled Resource Consumption	18-11-2019	7.8	Two memory leaks in the v3d_submit_cl_ioctl() function in drivers/gpu/drm/v3d/v3d_gem.c in the Linux kernel before 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering kcalloc() or v3d_job_init() failures, aka CID-29cd13cfd762.  CVE ID: CVE-2019-19044	N/A	O-LIN-LINU- 031219/149

Weakness	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIIPC ID
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the mlx5_fpga_conn_create_cq() function in drivers/net/ethernet/mella nox/mlx5/core/fpga/conn.c in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering mlx5_vector2eqn() failures, aka CID-c8c2a057fdc7.  CVE ID: CVE-2019-19045	N/A		O-LIN-LINU- 031219/150
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** A memory leak in theipmi_bmc_register() function in drivers/char/ipmi/ipmi_ms ghandler.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering ida_simple_get() failure, aka CID-4aa7afb0ee20. NOTE: third parties dispute the relevance of this because an attacker cannot realistically control this failure at probe time.  CVE ID: CVE-2019-19046	N/A		O-LIN-LINU- 031219/151
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the mlx5_fw_fatal_reporter_dum p() function in drivers/net/ethernet/mella nox/mlx5/core/health.c in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption) by	N/A		O-LIN-LINU- 031219/152
CV Scoring Scal (CVSS)	e 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			triggering mlx5_crdump_collect() failures, aka CID- c7ed6d0183d5.		
			CVE ID : CVE-2019-19047		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the crypto_reportstat() function in drivers/virt/vboxguest/vbo xguest_utils.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering copy_form_user() failures, aka CID-e0b0cb938864.	N/A	O-LIN-LINU- 031219/153
			CVE ID: CVE-2019-19048		
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** A memory leak in the unittest_data_add() function in drivers/of/unittest.c in the Linux kernel before 5.3.10 allows attackers to cause a denial of service (memory consumption) by triggering of_fdt_unflatten_tree() failures, aka CID-e13de8fe0d6a. NOTE: third parties dispute the relevance of this because unittest.c can only be reached during boot.  CVE ID: CVE-2019-19049	N/A	O-LIN-LINU- 031219/154
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the crypto_reportstat() function in crypto/crypto_user_stat.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service	N/A	O-LIN-LINU- 031219/155

4-5

5-6

6-7

8-9

9-10

7-8

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(memory consumption) by triggering crypto_reportstat_alg() failures, aka CID-c03b04dcdba1.  CVE ID: CVE-2019-19050		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the i2400m_op_rfkill_sw_toggle() function in drivers/net/wimax/i2400m /op-rfkill.c in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-6f3ef5c25cc7.  CVE ID: CVE-2019-19051	N/A	0-LIN-LINU- 031219/156
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the gs_can_open() function in drivers/net/can/usb/gs_usb .c in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering usb_submit_urb() failures, aka CID-fb5be6a7b486.  CVE ID: CVE-2019-19052	N/A	O-LIN-LINU- 031219/157
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the rpmsg_eptdev_write_iter() function in drivers/rpmsg/rpmsg_char.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering copy_from_iter_full() failures, aka CID-	N/A	O-LIN-LINU- 031219/158

4-5

6-7

5-6

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			bbe692e349e2.		
			CVE ID : CVE-2019-19053		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the cx23888_ir_probe() function in drivers/media/pci/cx23885 /cx23888-ir.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering kfifo_alloc() failures, aka CID-a7b2df76b42b.	N/A	O-LIN-LINU- 031219/159
			CVE ID : CVE-2019-19054		
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** A memory leak in the nl80211_get_ftm_responder_ stats() function in net/wireless/nl80211.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering nl80211hdr_put() failures, aka CID- 1399c59fa929. NOTE: third parties dispute the relevance of this because it occurs on a code path where a successful allocation has already occurred.  CVE ID: CVE-2019-19055	N/A	O-LIN-LINU- 031219/160
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the mwifiex_pcie_alloc_cmdrsp_buf() function in drivers/net/wireless/marve ll/mwifiex/pcie.c in the Linux kernel through 5.3.11 allows attackers to cause a	N/A	O-LIN-LINU- 031219/161

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (memory consumption) by triggering mwifiex_map_pci_memory() failures, aka CID-db8fd2cde932.  CVE ID: CVE-2019-19056		
Uncontrolled Resource Consumption	18-11-2019	7.8	Two memory leaks in the mwifiex_pcie_init_evt_ring() function in drivers/net/wireless/marve ll/mwifiex/pcie.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering mwifiex_map_pci_memory() failures, aka CID-d10dcb615c8e.  CVE ID: CVE-2019-19057	N/A	O-LIN-LINU- 031219/162
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the alloc_sgtable() function in drivers/net/wireless/intel/i wlwifi/fw/dbg.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering alloc_page() failures, aka CID-b4b814fec1a5.  CVE ID: CVE-2019-19058	N/A	O-LIN-LINU- 031219/163
Uncontrolled Resource Consumption	18-11-2019	7.8	Multiple memory leaks in the iwl_pcie_ctxt_info_gen3_init() function in drivers/net/wireless/intel/iwlwifi/pcie/ctxt-info-gen3.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service	N/A	O-LIN-LINU- 031219/164

4-5

5-6

6-7

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(memory consumption) by triggering iwl_pcie_init_fw_sec() or dma_alloc_coherent() failures, aka CID-0f4f199443fa.		
			CVE ID: CVE-2019-19059		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the adis_update_scan_mode() function in drivers/iio/imu/adis_buffer. c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-ab612b1daf41.	N/A	O-LIN-LINU- 031219/165
			CVE ID : CVE-2019-19060		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the adis_update_scan_mode_bur st() function in drivers/iio/imu/adis_buffer. c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-9c0530e898f3.  CVE ID: CVE-2019-19061	N/A	O-LIN-LINU- 031219/166
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the crypto_report() function in crypto/crypto_user_base.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering crypto_report_alg() failures, aka CID-ffdde5932042.  CVE ID: CVE-2019-19062	N/A	O-LIN-LINU- 031219/167

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID						
Uncontrolled Resource Consumption	18-11-2019	7.8	rtl_us drive: k/rtlv kerne attack service consu	nemory b_probe rs/net/v vifi/usb vifi/usb throug xers to ca ce (mem imption) 5169511 D: CVE-	() functivireless, c in the h 5.3.11 ause a doory, aka CII	on in /realte Linux allow enial of	N/A		O-LIN-L 031219	_						
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** A memory leak in the fsl_lpspi_probe() function in drivers/spi/spi-fsl-lpspi.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering pm_runtime_get_sync() failures, aka CID-057b8945f78f. NOTE: third parties dispute the relevance of this because an attacker cannot realistically control these failures at probe time.				N/A		0-LIN-L 031219							
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the sdma_init() function in drivers/infiniband/hw/hfi1 /sdma.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering rhashtable_init() failures, aka CID-34b3be18a04e.  CVE ID: CVE-2019-19065			N/A		0-LIN-L 031219								
Uncontrolled Resource	18-11-2019	7.8	A memory leak in the bfad_im_get_stats() function									IN/A			0-LIN-L 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10						

Weakness	Publish Date	CVSS	Description & CVE ID	Patc	h	NCIIPC ID
Consumption			in drivers/scsi/bfa/bfad_attr.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering bfa_port_get_stats() failures, aka CID-0e62395da2bd.  CVE ID: CVE-2019-19066			
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** Four memory leaks in the acp_hw_init() function in drivers/gpu/drm/amd/amd gpu/amdgpu_acp.c in the Linux kernel before 5.3.8 allow attackers to cause a denial of service (memory consumption) by triggering mfd_add_hotplug_devices() or pm_genpd_add_device() failures, aka CID-57be09c6e874. NOTE: third parties dispute the relevance of this because the attacker must already have privileges for module loading.  CVE ID: CVE-2019-19067	N/A		O-LIN-LINU- 031219/172
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the rtl8xxxu_submit_int_urb() function in drivers/net/wireless/realte k/rtl8xxxu/rtl8xxxu_core.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering usb_submit_urb() failures, aka CID-a2cdd07488e6.	N/A		0-LIN-LINU- 031219/173
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	ı	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			CVE I	D : CVE-	2019-19	9068				
Uncontrolled Resource Consumption	18-11-2019	7.8	fastrp functi driver Linux allow denia consu dma_{a} aka Cl	rs/misc/kernel bestacked of serving mption)get_sgtal	fastrpc.o fastrpc.o efore 5. ers to cau ce (men by trigg ble() fail a058d9	c in the 3.9 use a nory gering ures, 9.	N/A		O-LIN-L 031219	
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** A memory leak in the spi_gpio_probe() function in drivers/spi/spi-gpio.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering devm_add_action_or_reset() failures, aka CID-d3b0ffa1d75d. NOTE: third parties dispute the relevance of this because the system must have already been out of memory before the probe began.				N/A		O-LIN-L 031219	
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the rsi_send_beacon() function in drivers/net/wireless/rsi/rsi _91x_mgmt.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering rsi_prepare_beacon() failures, aka CID-			N/A		0-LIN-L 031219		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			d563131ef23c.		
			CVE ID: CVE-2019-19071		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the predicate_parse() function in kernel/trace/trace_events_fi lter.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-96c5c6e6a5b6.  CVE ID: CVE-2019-19072	N/A	O-LIN-LINU- 031219/177
Uncontrolled Resource Consumption	18-11-2019	7.8	Memory leaks in drivers/net/wireless/ath/at h9k/htc_hst.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering wait_for_completion_timeout () failures. This affects the htc_config_pipe_credits() function, the htc_setup_complete() function, and the htc_connect_service() function, aka CID-853acf7caf10.  CVE ID: CVE-2019-19073	N/A	O-LIN-LINU- 031219/178
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the ath9k_wmi_cmd() function in drivers/net/wireless/ath/at h9k/wmi.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-728c1e2a05e4.	N/A	O-LIN-LINU- 031219/179
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-19074		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the ca8210_probe() function in drivers/net/ieee802154/ca 8210.c in the Linux kernel before 5.3.8 allows attackers to cause a denial of service (memory consumption) by triggering ca8210_get_platform_data() failures, aka CID-6402939ec86e.	N/A	O-LIN-LINU- 031219/180
			CVE ID : CVE-2019-19075		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the nfp_abm_u32_knode_replace () function in drivers/net/ethernet/netro nome/nfp/abm/cls.c in the Linux kernel before 5.3.6 allows attackers to cause a denial of service (memory consumption), aka CID-78beef629fd9.  CVE ID: CVE-2019-19076	N/A	O-LIN-LINU- 031219/181
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the bnxt_re_create_srq() function in drivers/infiniband/hw/bnxt_re/ib_verbs.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering copy to udata failures, aka CID-4a9d46a9fe14.  CVE ID: CVE-2019-19077	N/A	O-LIN-LINU- 031219/182
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the ath10k_usb_hif_tx_sg() function in	N/A	O-LIN-LINU- 031219/183
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIIPC ID
			drivers/net/wireless/ath/at h10k/usb.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering usb_submit_urb() failures, aka CID-b8d17e7d93d2.			
			CVE ID : CVE-2019-19078			
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the qrtr_tun_write_iter() function in net/qrtr/tun.c in the Linux kernel before 5.3 allows attackers to cause a denial of service (memory consumption), aka CID-a21b7f0cff19.	N/A		O-LIN-LINU- 031219/184
			CVE ID : CVE-2019-19079			
Uncontrolled Resource Consumption	18-11-2019	7.8	Four memory leaks in the nfp_flower_spawn_phy_reprs () function in drivers/net/ethernet/netro nome/nfp/flower/main.c in the Linux kernel before 5.3.4 allow attackers to cause a denial of service (memory consumption), aka CID-8572cea1461a.  CVE ID: CVE-2019-19080	N/A		0-LIN-LINU- 031219/185
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the nfp_flower_spawn_vnic_repr s() function in drivers/net/ethernet/netro nome/nfp/flower/main.c in the Linux kernel before 5.3.4 allows attackers to cause a denial of service (memory consumption), aka CID-8ce39eb5a67a.	N/A		0-LIN-LINU- 031219/186
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 57	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID					
			CVE I	D : CVE-	2019-1	9081									
Uncontrolled Resource Consumption	18-11-2019	7.8	*create function driver ay/do urce.co dce10 function driver ay/do urce.co dce10 functive ay/do urce.co ard dce11 functive ay/do urce.co	10_create nction in rs/gpu/6 c/dce110 c, the 00_create rs/gpu/6 c, the 0_create ction in rs/gpu/6 c/dcn10	rce_poo er drm/am inux ker 1 allow ause a d ory 1. This af e_resour drm/am 0/dce12 e_resour drm/am 0/dce11 e_resour drm/am 0/dce10 _resourc drm/am /dcn10resourc drm/am /dcn10 e_resour drm/am /dcn10 e_resour drm/am	enial of fects fects fec_poo d/displ 0_reso fce_poo d/displ 0_reso fce_poo d/displ 0_reso fce_poo d/displ 0_reso fce_pool d/displ fects fce_pool d/displ fects fce_pool d/displ fce_pool d/displ fce_poo d/displ fce_poo	N/A		O-LIN-L 031219						
Uncontrolled	18-11-2019	7.8	Memory leaks in			•			-		I N/A			0-LIN-L 031219	
Resource			*clock_source_create()					001217	, 100						
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10					

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Consumption			functions under		
			drivers/gpu/drm/amd/displ		
			ay/dc in the Linux kernel		
			before 5.3.8 allow attackers		
			to cause a denial of service		
			(memory consumption).		
			This affects the		
			dce112_clock_source_create(		
			) function in		
			drivers/gpu/drm/amd/displ		
			ay/dc/dce112/dce112_reso		
			urce.c, the		
			dce100_clock_source_create(		
			) function in		
			drivers/gpu/drm/amd/displ		
			ay/dc/dce100/dce100_reso		
			urce.c, the		
			dcn10_clock_source_create()		
			function in		
			drivers/gpu/drm/amd/displ		
			ay/dc/dcn10/dcn10_resourc		
			e.c, the		
			dcn20_clock_source_create()		
			function in		
			drivers/gpu/drm/amd/displ		
			ay/dc/dcn20/dcn20_resourc		
			e.c, the		
			dce120_clock_source_create(		
			) function in		
			drivers/gpu/drm/amd/displ		
			ay/dc/dce120/dce120_reso		
			urce.c, the		
			dce110_clock_source_create(		
			) function in		
			drivers/gpu/drm/amd/displ		
			ay/dc/dce110/dce110_reso		
			urce.c, and the		
			dce80_clock_source_create()		
			function in		
			drivers/gpu/drm/amd/displ		
			ay/dc/dce80/dce80_resourc		

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID	
			e.c, ak	ka CID-0!	55e5474	ł78a1.					
			CVE I	D : CVE-	2019-1	9083					
Microsoft											
windows											
Untrusted Search Path	19-11-2019	6.9	Code42 app through version 7.0.2 for Windows has an Untrusted Search Path. In certain situations, a nonadministrative attacker on the local machine could create or modify a dynamiclink library (DLL). The Code42 service could then load it at runtime, and potentially execute arbitrary code at an elevated privilege on the local machine.  CVE ID: CVE-2019-16860				https://port.co .com/' s_and_ tions/ 42_cus r_suppresource ode42 rity_act ies/Ar y_code ution_ cal_Wi s_devices	ode42 Ferm condi Code stome oort_r ces/C _secu dvisor bitrar e_exec on_lo ndow	O-MIC-WIND- 031219/189		
Untrusted Search Path	19-11-2019	6.9	Code42 server through 7.0.2 for Windows has an Untrusted Search Path. In certain situations, a nonadministrative attacker on the local server could create or modify a dynamic-link library (DLL). The Code42 service could then load it at runtime, and potentially execute arbitrary code at an elevated privilege on the local server.				https:/ e42.co suppo E-201 16861	m/r/ rt/CV 9-	O-MIC-\ 031219		
Improper Privilege Management	18-11-2019	7.2	NVIDIA NVFlash, NVUFlash Tool prior to v5.588.0 and GPUModeSwitch Tool prior to 2019-11, NVIDIA kernel mode driver (nvflash.sys, nvflsh32.sys, and			N/A		O-MIC-\ 031219			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	:ch	NCIIP	C ID
			nvflsh64.sys) contains a vulnerability in which authenticated users with administrative privileges can gain access to device memory and registers of other devices not managed by NVIDIA, which may lead to escalation of privileges, information disclosure, or denial of service.  CVE ID: CVE-2019-5688							
phicomm			GVE	D. CVE	2017 5					
k2\(psg1218\)	\)_firmware									
Improper Input Validation	18-11-2019	9	/adm PHICO V22.5 remote to exe shell a cgi-bi	/usr/lib/lua/luci/controller /admin/autoupgrade.lua on PHICOMM K2(PSG1218) V22.5.9.163 devices allows remote authenticated users to execute any command via shell metacharacters in the cgi-bin/luci autoUpTime parameter.			N/A		O-PHI-K 031219	
Qualcomm										
qca6574au_fi	rmware									
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	varial firmw bound functi throu Auto, Snapo Electr Snapo Snapo Snapo	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in		https://w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA-031219	•	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 MSM8 QCA6 QCS40 SDM8	053, AP0 098, MD 3996AU, 574AU, 0 05, QCS6	0M9640, MSM89 QCN760 605, SDA	98, 5, 845,				
				D : CVE-						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	wlan rates elements than rates shaped Snaped Snaped Snaped APQ8 MDM MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81 CVE I	r overflomodule in or extendent length max rate dragon Aragon Conics Con	if suppo ded rate h is great set leng auto, compute consume onnective consume ndustria Mobile, Voice & M Q8053, MDM92 MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0 670, SD1 20, SM6 250, SXI	rted es ater eth in rity, r IOT, l IO	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	-
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,				https://w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	0-QUA- 031219	-
CV Scoring Scal	e 0-1	1-2	2-3			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 APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150  CVE ID: CVE-2019-2268	bulletin	
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-QCA6- 031219/196

Weakness	Publish Date	cvss	ı	Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
			SM81	50						
			CVE I	D : CVE-	2019-2	297				
qcs405_firmv	vare									
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack o will be modificated to will be modificated to will be modificated to wear and a second mobil Musica Wear and APQ8 MDM9 MDM9 MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM4 SDM6 SDM7 SDX24 SM81 CVE II	D : CVE-	ce lock werently e memorals to out in Snape gon Core onsume industria oT, Snape ragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905 MSM890	which  py t of dragon isumer ity, r IOT, dragon oice &  9,  8, 7C, 0, , 89, AU, CS605, 845, M630, M660, X20, 150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo 19- n	O-QUA- 031219	-
Improper Restriction of Operations	21-11-2019	2.1	varial firmw	oper vali ole receiv vare can d access	ved fron lead to o	n out of	https://ww w.qualcom m.com/com pany/produ		0-QUA- 031219	=
within the Bounds of a Memory			throu	on while gh loop i Snapdra	n Snapo	lragon	ct- security/bu lletins/octo		,	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	I	Description	on & CVE	Pat	ch	NCIIP	C ID	
Buffer			Electr Snapo Snapo Snapo APQ8 APQ8 MSM8 QCA6 QCS40 SDM8	lragon Conics Conics Colragon Indragon Words, APO 1998, MD 1996AU, 199	onnectiv Jonsume Idustria Jobile, Joice & M Q8096A MSM89 QCN760 605, SDA	ity, r IOT, l IOT, fusic in U, 98, 5, 845,	ber-20 bulleti			
Out-of- bounds Read	21-11-2019	4.6	Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in			https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,				https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin		O-QUA- 031219	-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	0-QUA-QCS4- 031219/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130		
			CVE ID : CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150  CVE ID: CVE-2019-2266	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-QCS4- 031219/202
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-QCS4- 031219/203
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch	NCIII	PC ID
			QCA9 SDA6 SDM6 SDM8	574AU, ( 379, QCS 60, SDM 60, SDM 45, SDX	5405, Q0 630, SD 670, SD 20, SM6	CS605, M636, M710, 150				
				<b>D : CVE-</b> nation d						
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	=
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing non- standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer				https://w.qual m.com pany/j	com /com	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150	security/bu lletins/octo ber-2019- bulletin	
in a 1010 firm			CVE ID : CVE-2019-2297		
ipq4019_firm	ware		Possible double free issue in		
Use After Free	21-11-2019	4.6	kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-IPQ4- 031219/206

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Desc	cription 8	k CVE I	Pat	ch	NCIIF	CID	
			QCA9980 SDM845, SM8150			-				
			CVE ID : 0	CVE-20	19-22	666				
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer ov while pro standard user space Auto, Sna Electronic Snapdrag Snapdrag Snapdrag Snapdrag Infrastruct Networki APQ8017 APQ8064 IPQ4019, MDM960 MDM965 MSM8990 QCA6574 QCA9379 QCS405, Q SDA845, SDM845, SDM845, SM8150	e from gon sumer ty, 10T, 10T, 10T, 10S, 28074, 25, 4A, 7, 1660, 44,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- 031219	-		
ipq8064_firm	ware									
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon				m.com pany/ ct- securi lletins ber-20	com /com produ ty/bu /octo	0-QUA- 031219	_
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3	70	1-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pate	ch	NCIIP	C ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150	bulletin	n		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8996AU, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297	https://w.qualm.com/pany/pct-securit lletins/ber-20 bulletin	com /com orodu y/bu /octo 19-	O-QUA-1 031219	-
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
ipq8074_firmware					
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-IPQ8- 031219/210
Out-of- bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-IPQ8- 031219/211
CV Scoring Scale (CVSS)	e 0-1	1-2	<b>2-3 3-4 4-5 5-6 72</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			APQ8 APQ8 MSM8 MSM8 MSM8 MSM8 QM21 SDM4	orking ir 053, AP( 096AU, 1 8917, MS 8937, MS 8953, MS 8996AU, 5, SDM4 1ragon_F	Q8096, IPQ8074 SM8920, SM8940, SM8996, QCA808 29, SDM	ł, 31, 1439,				
			CVE I	D : CVE-	2019-2	318				
qca6174a_firr	mware						1	Т		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	wlan rates elementhan rates shaped Snaped Snaped Snaped Snaped Snaped APQ8 APQ8 MDM MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	r overflomodule in or extendent length max rate dragon Aragon Coloragon Coloragon Maragon Mara	if suppoded rate his greaten set lenguto, ompute onsume on	rted es ater gth in r ity, r IOT, l IOT, dusic in 06, 07, , , , XS605, M710, 150, R2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com orodu xy/bu /octo 19-	0-QUA-0 031219	-
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN				https:/ w.qual m.com	com	0-QUA-0 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	ch	NCIIP	C ID			
			Snapo Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM9 MDM9 MSM8 QCA6 QCA9 SDA6 SDM8	gement for the second s	onsume onsume onsume dustria lobile, oice & M Q8017, Q8096A M9206, MDM960 SM8996 A6174A QCA937 S405, Q0 630, SD 6670, SD	er rity, er IOT, al IOT, Music in U, O7, SAU, A, CS605, M636, OM710, 150	pany/yct-securitilletins ber-20 bulleti	ty/bu /octo )19-		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer while stand user's Auto, Electric Snapo Snapo Snapo Infras Netwo APQ8 APQ8 IPQ40 MDM MDM MDM MSM8	r overflooprocessive NAN space. in Snapdra conics Codragon Indragon Maragon Warructure orking in 17, APC 19206, MI 19650, MI 1	w can o ing non- messag Snapdra igon Con onsume dustria lobile, foice & M Vired and a APQ80 Q8053, Q8096A B064, IP DM9640 SM8905 QCA617	ccur ge from agon nsumer rity, er IOT, al IOT, Music, Q8074, 7C, 0,	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			QCS40 SDA8	379, QCI 05, QCS6 45, SDM 445, SDX 50	636, SDA	M660,				
			CVE I	D : CVE-	2019-2	297				
qca9377_firm	ware									
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	wlan is rates element than is Snapo	r overflomodule in or extendent lengt in a rate dragon A dragon Conics Collagon Maragon Marago	if suppo ded rate h is grea set leng auto, compute consume onnectiv consume dobile, voice & N Q8053, MDM92 MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0 670, SDI 20, SM6	rted es ater eth in  r ity, er IOT, l IOT,  Music in  06, 07, , , , , AU,  CS605, M710, 150, R2130	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com orodu cy/bu /octo 19- n	0-QUA- 031219	-
Out-of- bounds Read	21-11-2019	7.5	P2P a handl mana Snapo Snapo Electr	ole OOB ction fra ing WLA gement f dragon A dragon C ronics Co	nmes wh AN frame in auto, consume onnectiv	ile er ity,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20	com /com orodu cy/bu /octo	0-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150  CVE ID: CVE-2019-2268	bulletin	
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-QCA9- 031219/217

qca9379_firmware    Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon, Mobile, Snabdragon, Mobile,	Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch:	NCIIP	C ID
Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Noice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9607, MDM9607, MDM9650, MSM8905, M											
Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Notice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8905				CVE I	D : CVE-	2019-2	297				
wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Notice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM89	qca9379_firm	iware									
P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT  P2P action frames while https://ww w.qualcom m.com/com pany/produ ct- security/bu O-QUA-QC 031219/2	without Checking Size of Input ('Classic Buffer	21-11-2019	4.6	wlan in rates element than in Snapo	module or extendent lengt max rate dragon Adragon Conics Coloragon Maragon Maragon Wolfragon Wol	if suppo ded rate h is grea set leng auto, compute consume onnectiv consume dobile, voice & N Q8053, MDM92 MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0 670, SDI 20, SM6	rted es ater gth in , or ity, er IOT, l IOT, Music in 06, 07, , CS605, M710, 150, R2130	w.qual m.com pany/ ct- securi lletins ber-20	com /com produ ty/bu /octo	=	_
Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017,		21-11-2019	7.5	P2P a handl mana Snapo Snapo Electr Snapo Snapo Snapo Snapo Snapo	ction fra ing WLA gement : dragon A dragon C dragon I dragon I dragon V	ames wh AN frame in Jonsume consume donsume dobile, Voice & M	ile r ity, r IOT, l IOT,	w.qual m.com pany/ ct- securi lletins ber-20	com /com produ ty/bu /octo	=	_
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9	_	e 0-1	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150  CVE ID: CVE-2019-2268		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	0-QUA-QCA9- 031219/220
apq8009_firm	nware				

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

Weakness	Publish Date	cvss		Descriptio	on & CVE	ID	Pat	ch	NCIII	PC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condit result in Sna Snapd Snapd Snapd Mobile Music Weara APQ86 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SDX59 SM818 Snapd	process messag tion is no ing into pdragor dragon C dragon Ic drag	te, Valid of met an infin in Auto, ompute onsume industria oT, Snaparagon Vagon APQ809 DM9607 DM9607 DM9655 DM9607 DM9655 DM8909, MSM8913, SM8953, SM8	exit ite loop , er IOT, l IOT, dragon oice & e9, 8, 5, 40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150, d_2016	https:/w.qualm.company/jct-securitelletins/ber-20bulleti	com /com produ ty/bu /octo	0-QUA 031219	•
Time-of- check Time- of-use (TOCTOU) Race	21-11-2019	4.4	lack of resource lock which will be concurrently w.qual m.com			lack of resource lock which will be concurrently modified in the memcpy w.qualcom m.com/com pany/produ		com /com	0-QUA 031219	-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Condition			Auto, Electr Snapo Snapo Snapo Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81	d access Snapdra conics Co dragon In dragon In dragon In dragon In e, Snapdr e, Snapdr ables in 1 017, APC 096AU, 1 9607, MI 9650, MS 8909W, I 8953, MS 8998, Nic 605, QCS 5, SDA6 129, SDM 10, SDM 10, SDM 10, SDM 10, SDM 10, SDM 10, SDM	agon Coronnective on sume and ustria of the coron of the	nsumer ity, er IOT, l IOT, dragon oice & 9, 8, 7C, 0, , 89, AU, CS605, 845, M630, M660, X20,	securit lletins ber-20 bulleti	/octo 119-		
Use After Free	21-11-2019	2.1	daeme static freed in Sna Snape Snape Snape Snape Mobil Music Wears APQ8	ter free on shute object in from a mapdragon Caragon Caragon Idragon I	lown dunstance grant program of the compute consume of the consumer of the co	e to getting places  , vity, er IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61 SM82	9207C, N 9650, MS 3909, MS 3917, MS 3937, MS 3940, MS 3996, MS 60, SDA8 60, SDA8 60, SDA8 50, SM7 50, SXR2	SM8905 SM8909' SM8939, SM8953, SM8996, Cobar, Q S45, SDM 2670, SD 20, SDX 2130	AU, CS605, 4450, M710, 24, 8150,				
Improper Validation of Array Index	21-11-2019	4.6	occur to imparray Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 SDX2		ra drive alidation Snapdrigon Coronsume dustria Mobile, foice & Moscore Moscor	r due n of agon nsumer ity, r IOT, l IOT, dusic, es in U, 07, 0, 17, 1898, 0M450, M660,	https:/w.qual m.com pany/ct- securif lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
Out-of-	21-11-2019	7.5	CVE ID : CVE-2019-10503  Possible OOB read issue in				https:/	//ww	O-QUA-	APQ8-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Descriptio	on & CVE	ID	Pat	ch	NCIIP	C ID
bounds Read			handl mana Snapo Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 MDM9 MDM9 MSM8 QCA6 QCA9 SDA6 SDM8	ction fra ing WLA gement f dragon A dragon C dragon C dragon M dragon W dragon W 009, APC 053, APC 098, MD 9207C, M 9650, MS 379, QCS 60, SDM 645, SDM 645, SDX	frame in auto, onsume o	r ity, r IOT, l IOT, Music in U, AU, A, 7, CS605, M636, M710,	w.qual m.com pany/p ct- securit lletins, ber-20 bulleti	/com produ ty/bu /octo 119-	031219	/225
Out-of- bounds Read	21-11-2019	10	while session messar un-information Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MDM MDM MD	r over reparsing parsing manages if netended valuagen Caragon Caragon Index, Snapdrables in April 206, MI 19206, MI 19615, MI 19635M, I I 19635M, I 19635M, I I 19635M, I I I I I I I I I I I I I I I I I I I	downlingement (etwork straines in uto, ompute, onsume ndustria oT, Snap ragon APQ800 Q8053, APQ809 DM9205 DM9607 DM9625	nk OTA ends  r IOT, l IOT, dragon oice &  9,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	NCIIP	C ID					
			MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	9650, MI 3905, MS 3909W, NS 3920, MS 3939, MS 3953, MS 3996AU, 45, SC818 45, SDM 45, SDM 10, SDM 10, SDM 50, SM7 50, 1ragon_H	5M8909, MSM8915, M8940, 5M8976, MSM89 2150, Q 80X, SD 429, SD 630, SD 660, SD 845, SD 845, SD	98, CS605, A660, M439, M632, M670, M850,				
Improper Authenticati on	21-11-2019	10	Lack of allow NAS in result bypas Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MDM MDM MD	D: CVE- of integrals s MODEN nessages c into aut as of NAS dragon A dragon C dragon Ic dragon Ic e, Snapdr ables in A 017, APC 096AU, A 9150, MI 9206, MI 9635M, I 9635M, I 9650, MI 3905, MS	ity check M to accombined to chentication in uto, ompute onsume of Saap ragon Vagon APQ800 Q8053, APQ809 DM9607 DM9607 DM9605 SM8909	ept any can tion  r IOT, dragon oice &  9, 8, 5, 40, 5,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA- 031219	_
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape Sna	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, SDM630,				//ww lcom produ ty/bu /octo 019- n	0-QUA- 031219	•
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM850, Snapdragon_High_Med_202, , SXR1130 CVE ID: CVE-2019-2295	16	
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT Snapdragon Industrial IOT Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ807 MDM9206, MDM9207C, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660 SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8- 031219/229
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragod Auto, Snapdragon Computer Snapdragon Consumer IOT Snapdragon Industrial IOT Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice of	w.qualcom m.com/com pany/produ e, ct- r, security/bu lletins/octo ton ber-2019-	O-QUA-APQ8- 031219/230
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6 6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	c, Snapdrables in 2017, APC 096AU, 29150, MI 9615, MI 9635M, II 9650, MI 3905, MS 3909W, II 3939, MS 3939, MS 3939, MS 3953, MS 3909W, II 300, SDX24 50, SDM 100, SDX24 500, SM7 100, SDX24 500, SM7 100, SM7	APQ800 Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 GM8909, MSM8937, GM8976, MSM8976, MSM89, Q150, Q0 80X, SDA 429, SDI 1630, SD 1845, SD 150, SM High_Me R2130	8, 5, 7, 40, 5, 40, 5, 7, 27, 27, 28, 28, 28, 28, 38, 46, 46, 46, 46, 48, 50, 61, 61, 61, 61, 61, 61, 61, 61, 61, 61				
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
apq8098_firn	iware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-APQ8- 031219/232

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch:	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9650, MI 3905, MS 3909W, NS 3920, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDM 530, SDM 545, SDM 545, SDM 550, SM83 1ragon_H	5M8909, MSM8915, SM8953, SM8996, cobar, S605, Q 6632, SD 6632, SD 6670, SD 6850, SD 50, SM72 250,	AU, M215, A845, M450, M636, M710, X20,				
			CVE I	D : CVE-	2019-2	335				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605,				https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description & CVE ID				ch	NCIIP	C ID
			SDM4 SDM6 SDM7 SDX2	QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150						
			CVE I	D : CVE-	2019-1	0486				
Use After Free	21-11-2019	2.1	freed in Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61 SM82	static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA645, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130  CVE ID: CVE-2019-10490				//ww com /com produ ty/bu /octo 19- n	O-QUA- 031219	•
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of				https:/ w.qual m.com	com	0-QUA- 031219	-
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			array index in Snapdragon Auto, 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, MSM8905, MSM8909, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503	pany/produ ct- security/bu lletins/octo ber-2019- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8996AU, QCA6574AU, QCN7605, QCS405, QCS605, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8- 031219/236

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	CID
			SDM8	45, SDX	20					
			CVE I	D : CVE-	2019-1	0535				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID: CVE-2019-2251				https://w.qualm.com pany/jct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017,				https://w.qualm.com/pany/jct-securifiletins/ber-20	com /com produ ty/bu /octo	0-QUA- 031219	_
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

APQ8093, APQ8096AU, APQ8096, MDM9207C, MDM9650, MDM9207C, MDM9650, MSM8996AU, MSM8996, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM630, SDM630, SDM630, SDM630, SDM650, MSM6909, MSM69050, MSM69050, MSM69050, MSM89050, MSM89	Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	CID
Out-of-bounds Read         21-11-2019         10         While parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8098, MUSIC, Snapdragon Wearables in APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9206, MDM9607, MDM9615, MDM9625, MDM963M, MDM9655, MSM8909, MSM890, MSM8917, MSM8996AU, MSM8937, MSM8996AU, MSM8998, Nicobar, QCM215, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,         0-QUA-APQ8-031219/239           CV Scoring Scale         0.1         1.2         23.4         3.4         4.5         5.6         6.7         7.8         8.9         9.10				APQ8 MDM9 MSM8 QCA6 QCA9 SDA6 SDM6 SDM8	098, MD 9207C, M 9650, M 3998, QC 574AU, ( 379, QC 60, SDM 445, SDX	M9206, 4DM960 5M8996 A6174A QCA937 5405, QC 630, SDI 6670, SD	07, AU, 7, CS605, M636, M710,				
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		21-11-2019	10	while session messar un-interpretation of the session messar un-interpretation of the session messar un-interpretation of the session messar session of the session of the session messar appearance which was appearance with the session of the sess	parsing on manage deges if not dragon A dragon I dragon I	downlingement (etwork stalues in uto, ompute onsume ndustrial of Sagon Vagon V	nk OTA rends r IOT, l IOT, dragon foice & 9, 8, 6, 7, 6, 40, 6, 40, 6, 47, CS605, A660, M439,	w.qual m.com pany/i ct- securit lletins ber-20	ty/bu /octo	•	•
	_	e	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			SDM7 SDX2 SM61 SM82 Snapo	36, SDM 10, SDM 0, SDX24 50, SM7 50, dragon_H 1130, SX <b>D : CVE-</b>	845, SD 2, SDX55 150, SM High_Me R2130	M850, , 8150, d_2016				
Improper Authenticati on	21-11-2019	10	allow NAS result bypas Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM' MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDM8 SDM6 SDM7	of integrals MODEI nessages into autoris of NAS dragon A dragon Idragon Idrago	M to access which of thentical sin auto, ompute, onsume adustria oT, Snap aragon Vagon APQ800 DM9625 DM8937, SM8940, SM8940, SM8940, SD630X, SD6429, SD6430, SD64300, S	ept any can cion cion r IOT, l IOT, dragon oice & 9, 8, 7, 7, 140, 17, 17, 186, 186, 186, 186, 186, 186, 186, 186	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA- 031219	•
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1	1 2	2 3	- J -	7 3	3 0	3 /	, 0	0 9	J 10

			Description & CVE ID	Patch	NCIIPC ID
Out-of-	21-11-2019	7.5	SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289  SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MDM9650, MDM9655,	https://ww w.qualcom m.com/com pany/produ ct-	O-QUA-APQ8-
Out-of- bounds Read	21-11-2019	7.5	MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	w.qualcom m.com/com pany/produ	O-QUA-APQ8- 031219/241

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, APQ8098, MDM9150, SDM630, SDM630, SDM632, SDM636, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2315	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-APQ8- 031219/242
msm8939_fir	inwai e		Describer 1 et al	1.44	O-QUA-
Time-of- check Time- of-use	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently	https://ww w.qualcom m.com/com	MSM8- 031219/243
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6 95</b>	6-7 7-8	8-9 9-10

modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8096AU, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM632, SDM636, SDM660, SDM710, SDM845, SDX24, SM6150, SM7150, SM8150  CVE ID : CVE-2019-10486  Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Compute, Snapdragon Compute, O-QUA-	Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute,  https://ww w.qualcom m.com/com pany/produ O-OUA-	Race			statent bound Auto, Electr Snape Snape Snape Mobil Music Weard APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81	nent lead d access Snapdra conics Co dragon Id dragon Id dragon Id e, Snapdra bles in 1 017, APO 096AU, 1 9206, Mi 9650, Mi	ds to our in Snape agon Coronnective Consume adustria oT, Snape dragon Veragon APQ800 DM9207 DM9640 SM8905 MSM8935 GM89964 Cobar, S405, Quantum 1439, SDA 1439, SDA 1439, SDA 1636, SDA 16	t of dragon asumer ity, or IOT, l IOT, dragon foice &  9,  8, 7C, 0, , 39, AU, CS605, 845, M630, M660, X20, 150,	ct- securit lletins ber-20	ty/bu /octo )19-		
Free  21-11-2019 2.1 Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,  MSM8- 031219/244	Use After Free	21-11-2019	2.1	daeme static freed in Snapo Snapo Snapo Snapo Snapo Mobil Music Weara	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,				com /com produ ty/bu /octo	MSM8-	/244
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8993, MSM8994, MSM8996, MSM8996AU, MSM8996, MSM8906AU, MSM8996, MSM8906AU, MSM8996, MSM8906AU, MSM8996, MSM8906AU, MSM8950, SDM450, SDM450, SDM660, SDM670, SDM710, SDM660, SDM670, SDM710, SDM660, SDM670, SDM710, SM8250, SXR2130  CVE ID : CVE-2019-10490  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Orosumer IOT, Snapdragon IOT, Snapdragon Mobile, Snapdragon wearables in APQ8009, MSM9096AU, APQ8098, MDM9150, MDM9205, MDM9150, MDM9205, MDM9150, MDM9205, MDM9615, MDM9620, MDM9615, MDM9620, MDM9655, MSM8909, MSM8909W, MSM8917, MSM8920, MSM89917, MSM8920, MSM89940, MSM8933, MSM8976,  CV Scoring Scale  0,1 12 2,3 3,4 4,5 5,6 6,7 7,8 8,9 9,10	Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	tch	NCIIP	C ID
Out-of-bounds Read  Out-of				MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> SDA <sup>o</sup> SDM <sup>o</sup> SDM <sup>o</sup> SM <sup>o</sup> SM <sup>o</sup> SM <sup>o</sup> SM <sup>o</sup>	9150, MI 9207C, M 9650, MS 8909, MS 8917, MS 8937, MS 8996, MS 8996, MS 60, SDM 60, SDM 645, SDX 50, SM7	DM9206 ADM960 SM8905 SM8909 SM8939, SM8953, SM8956, SM8956, SM8956, SM8956, SM8956, SM8956, SM8956, SM8956, SM8936, SM896,	5, 07, , , W, CS605, , M710, 24, 8150,				
while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9205, MDM9607, MDM9607, MDM9607, MDM9605, MDM9607, MDM9605, MDM9605, MDM9605, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8917, MSM8939, MSM8940, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976,											
-		21-11-2019	10	while session messar un-interpretation of the session messar un-interpretation of the session messar of the session of the ses	Buffer over read can happen while parsing downlink session management OTA messages 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, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909W, MSM8909, MSM8909W, MSM8909M, MSM890M, MSM89		w.qual m.com pany/i ct- securit lletins ber-20	lcom l/com produ ty/bu /octo	MSM8-	/245	
(1)	CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016
, SXR1130, SXR2130 CVE ID : CVE-2019-2271
Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ805, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9650, MDM96650, MDM9650, MDM9650, MDM9650, MDM9650, MDM9650, MDM9650, MDM96650, MDM9650, MDM9650, MDM9650, MDM96650, MDM9665
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1

			SDM4 SDM6	45, SDM 50, SDM 36, SDM	•	•				
			SM61 SM82 Snapo , SXR1	10, SDM 0, SDX24 50, SM7	1660, SD 1845, SD 1, SDX55 150, SM High_Med R2130	M670, M850, , 8150, d_2016				
Out-of-bounds Read 2	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Weara APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	P modulout side it receive lessage. It says a largon Caragon In largon In la	its bour res malfo in Snapo agon Cor onsume dustria oT, Snapo ragon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9625 MSM8909, MSM8916,	ndary ormed lragon inpute, or IOT, loot, l	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219,	/247
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
msm8953_fir	mware		SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MSM8- 031219/248

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			, SXR1	130, SX	R2130					
			CVE I	D : CVE-	2019-2	335				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated bound Auto, Electron Snape Snape Snape Mobil Music Wears APQ8 MDM MDM MDM MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX2 SM81	condition f resour e concur fied in the ment lead d access Snapdra conics Col dragon In dragon I	ce lock verently the memory ds to out in Snape agon Corr onnective consume adustria oT, Snape lragon Veragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905	which  py t of dragon isumer ity, r IOT, dragon oice &  9,  8, 7C, 0, , 89, AU, CS605, 845, M630, M660, X20, 150,	https:/w.qualm.company/jct-securitiletins.ber-20	ty/bu /octo	O-QUA- MSM8- 031219	/249
			Use at	fter free	issue in	Xtra	https:/	,		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,				w.qual m.com pany/j ct- securit lletins ber-20	ty/bu	O-QUA- MSM8- 031219	/250
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM896AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450,
SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490
Improper Validation of Array Index  Array Index  Array Index  Array Modes  Array Index   Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, 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, MSM8905, MSM8909, MCM0000W, MCM0017
MSM8909W, MSM8917, MSM8920, MSM8937,

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 QCN7	3940, MS 3996AU, 605, SD 330, SDM 0	MSM89 A660, SI	98, 0M450,				
			CVE I	D : CVE-	2019-1	0503				
Out-of- bounds Read	21-11-2019	10	while session messar un-in Snapo Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	r over reparsing on manages if no tended with a gon of the gon of	downlingement (etwork straines in auto, ompute, onsume adustria oT, Snaphragon Vagon APQ800 DM9605 D	nk OTA ends r IOT, l IOT, dragon foice & 9, 8, 5, 40, 5, 40, 5, 47, 40, 6, 40, 6, M439, M632, M670, M850,	https:/w.qualm.company/jct-securitalietinsber-20bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/252
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, SDM850, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MSM8- 031219/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130  CVE ID: CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MSM8- 031219/254
			SNDCP module may access	https://ww	
Out-of- bounds Read	21-11-2019	7.5	array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/255

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
V CUMICSS			Weara APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	ables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 3905, MS 3905, MS 3905, MS 3939, MS 3953, MS 3	APQ800 Q8053, APQ809 DM9205 DM9607 DM9655 MDM9655 SM8909, MSM8916, SM8976, MSM89 2150, Q0 80X, SDA 429, SDI 1630, SD 1660, SD 1660, SD 1845, SD 150, SM High_Me R2130	9, 8, 6, 7, 40, 6, 7, 98, CS605, A660, M439, M632, M670, M850, , 8150, d_2016			, veill	
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	/256
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch.	NCIIP	C ID
			APQ8 APQ8 MDM <sup>1</sup> MSM8 MSM8 MSM8 MSM8 QCS4 <sup>1</sup> SDM6 SDM6 SDM6 SDM8 SM81 Snapo , SXR1	lragon_H I 130, SXI	Q8096A M9150, DM9206 DM9650 SM8909, SM8940, SM8946, MSM89 605, QM: S450, SDM 450, SDM 150, SM	5, 0, 98, 215, M429, M630, M660, M845, 7150,				
Out-of- bounds Read	21-11-2019	2.1	Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096,			https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/257	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016		
			CVE ID : CVE-2019-2318		
msm8998_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	0-QUA- MSM8- 031219/258

Weakness	Publish Date	CVSS	[	Description	n & CVE	ID	Pat	ch	NCIII	PC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated bound Auto, Electric Snaped Snaped Snaped Mobile Weara APQ86 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 SDM1 SDM4 SDM6 SDM7 SDX24 SM81	condition f resource e concur ied in the nent lead d access a Snapdra onics Co lragon Id ragon Id ragon Id ragon Id ragon Id solor, APC 096AU, A 017, APC 096AU, A 0206, MI 0607, MI 0607, MI 0607, MI 0607, MI 0650, MS 0998, Nid 0650, QCS 5, SDA6 29, SDM 10, SDM 10, SDM 11, SM615 50 D: CVE-	ce lock werently e memorals to our in Snaporals gon Corrective onsume industria oT, Snaporagon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905 MSM89	which  py t of dragon isumer ity, r IOT, dragon oice &  9,  8, 7C, 0, , 89, AU, CS605, 845, M630, M660, X20, 150,	https:/ w.qual m.com pany/p ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	
Use After Free	21-11-2019	2.1	daemo static freed in Sna Snapd Snapd Snapd Snapd Snapd	ter free on shutd object ir from a nepdragor Caragon Caragon Iragon Iragon Iragon Icagon Icag	lown dunstance production Auto, compute connectionsume adustria or, Snap	e to getting places , vity, r IOT, l IOT, dragon	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			Wears APQ8 APQ8 MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM8 SM61	c, Snapdr ables in A 017, APC 096AU, A 9150, MS 9207C, M 9650, MS 3909, MS 3997, MS 3996, MS 3996, MS 3998, Nic 60, SDAS 60, SDAS 50, SXR2	APQ800 Q8053, APQ809 DM9206 MDM960 SM8905 SM8909 SM8939, SM8939, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953,	8, 5, 07, W, W, AU, CS605, M450, M710,				
			CVE I	D : CVE-	2019-1	0490				
Improper Validation of Array Index	21-11-2019	4.6	occur to imparray Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8909W, MSM8937, MSM8940, MSM8953, MSM8940, MSM8998,				//ww lcom n/com produ ty/bu /octo 019- n	O-QUA- MSM8- 031219	/261
CV Scoring Scale (CVSS)	e <b>0</b> -1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDX2	30, SDM 0	636, SD	M660,				
			CVE I	D : CVE-	2019-1	0503				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20  CVE ID: CVE-2019-10535  Buffer over-read can occur in fast message handler due				https:/ w.qual m.com pany/i ct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA- MSM8- 031219	/262
Out-of- bounds Read	21-11-2019	4.6	in fast to imp while from Snapo Snapo Snapo Snapo Snapo Snapo APQ8 MSM8 QCN7	SDM845, SDX20  CVE ID : CVE-2019-10535  Buffer over-read can occur				//ww lcom l/com produ ty/bu /octo )19- n	0-QUA- MSM8- 031219	/263
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID: CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MSM8- 031219/264
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/265

4-5

6-7

5-6

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			MDM <sup>o</sup> MSM8 QCA6 QCA9 SDA6 SDM6 SDM8	098, MD 9207C, M 9650, MS 3998, QC 574AU, G 379, QCS 60, SDM 660, SDM 445, SDX	1DM960 5M8996 A6174A QCA937 5405, QC 630, SDI 670, SD 20, SM6	AU, 7, 2S605, M636, M710,				
Out-of- bounds Read	21-11-2019	10	while session messar un-introduction Snapor Snapor Snapor Snapor Snapor Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	r over reparsing on manages if netended valuages if netended valuagen Caragon Caragon Indicates in Automotive, Snapdrables in Automotive, Snapdrables, MI 19635M,	downlingement (sement	nk OTA ends  r IOT, l IOT, dragon oice &  9,  8,  7,  40,  7,  25605, A660, M439, M632,	https://w.qualm.company/jct-securitelletins/ber-20	com /com produ ty/bu /octo	O-QUA- MSM8- 031219,	/266
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDX2 SM61 SM82 Snapo	10, SDM 0, SDX24 50, SM7 50, dragon_F 1130, SX <b>D: CVE-</b>	I, SDX55 150, SM Iigh_Me R2130	, 8150, d_2016				
Improper Authenticati on	21-11-2019	10	allow NAS r result bypas Snapo Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musio Wear APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integrals MODEL nessages into autoris of NAS dragon A dragon In	M to accion which chenticals in auto, compute consume adustria of the consume and striagon Wagon APQ800 DM9605 DM9	ept any can tion from tion, r IOT, dragon foice & 9, 8, 5, 7, 6, 40, 6, 7, 40, 6, 4660, 4439, 4660, 46	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA- MSM8- 031219	/267
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	1	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			, SXR1	50, dragon_H 1130, SX <b>D : CVE-</b> nation d	R2130 <b>2019-2</b>	289				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	check buffer Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 Snapo CVE I	lragon_I l 130 <b>D : CVE-</b>	the System the System the System to the Syst	DBG, vity, r IOT, l IOT, fusic, 09, CS404, 215, M429, M630, M660, M845, d_2016	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo 119- n	0-QUA- MSM8- 031219	/268
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo	SNDCP module may access array out side its boundary w.qualcom when it receives malformed XID message. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, lletins/octo				com /com produ	O-QUA- MSM8- 031219	/269
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	lragon Ide, Snapdrables in 2017, APC 096AU, APC 096AU, APC 09650, MS 09650, MS 0996AU, APC 096AU, A	lragon V ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MB9655 GM8909, MSM891 SM8937, SM8940, SM8976, MSM89 2150, Qu 80X, SDA 429, SDA 1630, SDA 1640, SDA 1650, SDA 1650, SDA	oice & 9, 8, 5, 40, 5, 4660, M439, M632, M670, M850, 5, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	ber-20 bulleti			
N/A	21-11-2019	7.2	copy for the to the Paramare from environment Auto, Snapo Snapo Snapo Snapo	invoking from fd of secure lands on secure lands on secure lands on the secure lands o	or local bouffer, eing popsecure in Snapengon Cortonsumendustria Mobile,	ouffer oulated dragon npute, vity, r IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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, MSM8953, MSM8996, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
nicobar_firm	ware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-NICO- 031219/271

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9615, MI 9635M, I 9635M, I 9650, MS 8905, MS 8920, MS 8940, MS 8976, MS 80X, SDA 2150, QC 80X, SDM 530, SDM 545, SDM 545, SDM 545, SDM 545, SM615 50, SM82 dragon_H	MDM9655 M8909, MSM8915 M8953, M8953, M8996, Cobar, S605, Q 6632, SD 6632, SD 6670, SD 6630, SM7 250, High_Me R2130	40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150,				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race of lack of will be modified to the state of the stat	condition of resource concurfied in the ment lead access in Snapdra conics Codragon Codragon Indragon	n due to ce lock we rently e memo ds to out in Snapo agon Cor onsume out, Snapo aragon V ragon APQ800 Q8053, APQ809 DM9640 SM8905 MSM893	the which rpy t of dragon sumer ity, odragon roice & r	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			QCN7 QM21 SDM4 SDM6 SDM7	3998, Nio 605, QC 5, SDA6 29, SDM 32, SDM 10, SDM 4, SM615	5405, Q0 60, SDA 439, SD 636, SD 845, SD	845, M630, M660, X20,				
			Use at	<b>D : CVE-</b> fter free on shutd	issue in	Xtra				
Use After Free	21-11-2019	2.1	freed in Snape Snape Snape Snape Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM8 SM61 SM82	object ir from a mapdragon Calragon Calragon Calragon In Idragon I	nultiple n Auto, ompute onnective onsume ndustria oT, Snap ragon V agon APQ800 Q8053, APQ809 OM9206 M8905 M8905 M8905 M8905 M8960 SM8953, SM89	places  vity, r IOT, l IOT, dragon oice &  9,  8, 7, , W, CS605, M450, M710, 24, 8150,	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Buffer Copy	21-11-2019	4.6	Buffer	r overflo	w can o	ccur in	https:/	//ww	O-QUA-	NICO-
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

	Publish Date	cvss	[	Descriptio	n & CVE	ID	Pat	ch	NCIIP	CID
without Checking Size of Input ('Classic Buffer Overflow')			rates of elements of than response of the stranged Snaped Snaped Snaped Snaped APQ8 MDM9 MDM9 MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	or extendinated raginal raginated ra	ompute, onsume onsume dustrial lobile, loice & M Q8053, MDM920 MDM960 SM8905, Nicobar CA6574A	s ter th in rity, r IOT, IOT, IOT, AU, CS605, M710, 150, R2130	w.qual m.com pany/j ct- securit lletins ber-20 bulleti	/com produ ty/bu /octo 019-	031219	/274
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from a source that the potent buffer Snaped	any un-a e, there i ne bitma tially cau roverfloo lragon C lragon C lragon C lragon C lragon C lragon M	use stack w. in uto, ompute, onnective onsume onsume industrial	cated ibility	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-1 031219	
			APQ8	•	Q8096AU	IJ,				

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			Nicob SA61! SDA8- SDM6 SDM8 SM61 SM82	3996AU, ar, QCS4 55P, SC8 45, SDM 45, SDM 50, SM7 50, SXR2	:05, QCS 180X, SI 630, SDI (670, SD (850, SD 150, SM	605, DA660, M636, M710, X24, 8150,				
Use After Free	21-11-2019	4.6	kerne camer modu Snapo Snapo Snapo Mobil Musio Wears Wired Netwo IPQ40 MDM9 MDM9 MSM8 QCA9 SDM8 SM81	ole double while he sensor les power largon Aragon Infragon Infragon Infrastro la	r and ing r and its er seque uto, onsume ndustria oT, Snap ragon apdrago ructure a APQ80 S064, DM9207 SM8909 Nicobar, S405, Q0	the sub ence in IOT, I IOT, dragon foice & On and 53, 7C, 150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Out-of- bounds Read	21-11-2019	10	while session messa un-int Snapo Snapo Snapo Snapo	r over re parsing on manag ges if ne tended v Iragon C Iragon C Iragon I	downlingement of the second se	nk OTA eends , rr IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Music Wears APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM4 SDM6 SDM7 SDX2 SM61 SM82 SM61 SM82 SM82 SM82 SM82 SM82 SM82	lragon_H I 130, SX <b>D : CVE-</b>	ragon APQ800 Q8053, APQ809 DM9205 DM9607 DM9655 MDM9655 SM8909, MSM891 SM8940, SM8940, SM8940, SM8940, SM8956, Q0150, Q0 1660, SD 1660, SD 1660, SD 1660, SD 1645, SD 150, SM	9, 8, 5, 40, 5, 40, 5, 47, 28, 5, 6605, M439, M632, M670, M850, , 8150, d_2016				
Improper Authenticati on	21-11-2019	10	allow NAS result bypas Snapo Snapo Snapo Snapo Snapo Mobil Musio	of integrows MODEI sees ages sinto autorises of NAS dragon A dragon Collegon In dragon In	M to accombined to accombine the compute on sume on the combine th	ept any can tion r IOT, l IOT, dragon oice &	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	CID
			APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MI 3905, MS 3909W, I 3920, MS 3939, MS 3939, MS 3953, MS 3953, MS 3953, MS 3053, MS 305	APQ809 DM9205 DM9607 DM9625 MDM9655 SM8909, MSM891 SM8940, SM8940, SM8976, MSM89 2150, Qu 80X, SDA 429, SDI 1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	5, 7, 6, 40, 5, 17, 98, CS605, A660, M439, M632, M670, M850, 5,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape APQ8	nation d k of addr done or rs in SDI dragon C dragon C dragon I dragon W dragon W dragon W dragon W dragon W dragon W dragon W	ress range the System the System to the Syst	ge sDBG  vity, or IOT, I IOT, Music,	https://w.qualm.com/pany/jct-securitelletins/ber-20	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	I	Descriptio	n & CVE	ID	Pat	ch	NCIIP	CID
			MSM8 MSM8 QCS46 SDA66 SDM6 SDM6 SDM8 Snapo	lragon_H	M8937, M8953, cobar, Q 05, QM2 345, SDM 450, SD 636, SD 710, SD	CS404, 215, 4429, M630, M660, M845, d_2016				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Musio Weara APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8 MSM8	P modul out side it receives age. is Snapdra dragon Ic dragon, MI 9615, MI 9635M, Ic dragon, MS 9650, MS 9650, MS 9639, MS 9639, MS 9639, MS 9639, MS 9639, MS 9653, MS	e may active malforms	ccess idary ormed dragon inpute, r IOT, dragon oice &  9,  8,  6,  7,  7,  98,  CS605, A660, M439,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-1 031219	
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	,	,					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
	S S S S S		SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID: CVE-2019-2303		
apq8053_firm	nware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-APQ8- 031219/281

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SM81 Snapo	5, SM61! 50, SM8 lragon_F l130, SX	250, Iigh_Me					
			CVE I	D : CVE-	2019-2	335				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated bound Auto, Electron Snape Snape Snape Mobil Music Wears APQ8 MDM MDM MDM MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX2 SM81	condition of resour e concur fied in the nent lead d access Snapdra conics Co dragon In dragon I	ce lock werently the memorals to our in Snape agon Core onnective onsume adustria oT, Snape lragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905 MSM8905 G0, SDA (439, SD (636, SD (636, SD (636, SD (636, SD (636, SD	which rpy t of dragon nsumer ity, r IOT, l IOT, dragon oice & r 7, 8, 7, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	•
Use After Free	21-11-2019	2.1	daem static freed	fter free on shutc object in from a m apdragon	lown du istance ; nultiple	ue to w.qualcom getting m.com/con			0-QUA 031219	•
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Snapo Snapo Snapo Snapo Mobil Music Weara APQ8 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDA66 SDM6 SDM6 SDM6 SDM8	lragon C dragon C dragon I dragon I dragon I dragon I dragon I e, Snapdr ables in I 017, APC 096AU, I 9150, MS 9207C, M 9650, MS 3909, MS 3909, MS 3917, MS 3937, MS 3940, MS 3996, SDAS 50, SDAS 50, SM7	connective on sume and ustrial off, Snap bragon APQ800 Q8053, APQ809 DM960 SM8905 SM8905 SM8939, SM8953, SM8956, SM895	vity, er IOT, el IOT, edragon oice & e9, 8, 5, 77, , W, , AU, CS605, M450, M710, 24, 8150,	securit lletins ber-20 bulleti	octo 19-		
Improper Validation of Array Index	21-11-2019	4.6	occur to imp array Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM	f-bounds in came proper v index in Snapdra conics Co dragon In dragon V dragon V 009, APO 053, APO 098, MD 9207C, M	ra drive alidation Snapdr Igon Cor Innectiv Ionsume Industria Mobile, Yoice & M Vearable Q8017, Q8096A M9206, MDM960	er due n of agon nsumer ity, er IOT, l IOT, usic, es in U,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch:	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 QCN7	3905, MS 3909W, I 3920, MS 3940, MS 3996AU, 605, SDA 30, SDM	MSM891 SM8937, SM8953, MSM89 A660, SI	.7, 98, 0M450,				
			CVE I	D : CVE-	2019-1	0503				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	varial firmw bound functi throu Auto, Snapo Snapo Snapo APQ8 APQ8 MSM8 QCA6 QCS44 SDM8	oper valiole receivare can di accession while gh loop is Snapdradragon Chagon Chagon Maragon Wobsa, APO 1998, MD 1996AU, 1996A	ved from lead to o in WLAI e iteratin in Snapo agon Cor onsume onnectiv onsume dobile, oice & M Q8096A MSM89 QCN760 505, SDA 20	n out of N ng lragon npute, r ity, r IOT, l IOT, U, 98, 5,	https:/ w.qual m.com pany/j ct- securif lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA 031219	•
Out-of- bounds Read	21-11-2019	4.6	in fast to imp while from Snapo Snapo Electr Snapo Snapo	r over-re t messag process firmwar dragon A dragon C dragon C dragon I dragon M	ge handlo nput vali ing a me e in outo, onsume onnectiv onsume ndustria	er due idation essage r ity, r IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8- 031219/287
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-	0-QUA-APQ8- 031219/288
CV Scoring Scale (CVSS)	e 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			Music Wears Wired Netwo IPQ40 MDM' MDM' MSM8 QCA9 SDM8 SM81	e, Snapdr c, Snapdr ables, Sn d Infrastr orking ir 019, IPQ8 9206, M1 9607, M1 980, QC8 145, SDX 50 <b>D: CVE-</b>	ragon apdrago ructure a APQ80 8064, DM9207 SM8909 Nicobar, S405, Q0	on and 53, 7C, , CS605, 150,	bulleti	n		
Out-of- bounds Read	21-11-2019	7.5	P2P a handl mana Snapo Snapo Snapo Snapo APQ8 APQ8 MDM MSM8 QCA6 QCA9 SDA6 SDM8	ole OOB ction fra ing WLA gement if dragon A dragon C dragon C dragon M dragon W 009, APC 053, APC 098, MD 9207C, M 9650, MS 379, QC 574AU, C 379, QC 574AU, C 379, QC 574AU, C 574AU,	imes whan frame in tuto, consume connective consume dobile, Goice & M Q8017, Q8096A M9206, MDM960 SM8996 CA6174A QCA937 S405, QC 630, SDI 1670, SD 20, SM6	ile  ir ity, ity, I IOT, I IOT, Ausic in  U, 7, AU, A, 7, CS605, M636, M710, 150	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
Out-of- bounds Read	21-11-2019	10	while sessio	over re parsing on manag ages if ne	downlir gement (	nk OTA	https://ww w.qualcom m.com/com pany/produ		0-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	PC ID
			un-in	tended v	alues in		ct-			
			Snapo	dragon A	uto,		securi	ty/bu		
			Snapo	dragon C	ompute,	•	lletins	octo/		
			_	dragon C			ber-20			
			_	dragon Ir			bulleti	n		
			Snapo	dragon Io	T, Snap	dragon				
			Mobil	e, Snapd	ragon V	oice &				
				:, Snapdr	_					
				ables in A	•	9,				
			•	017, AP0	•					
			•	096AU,	•					
				9150, MI						
				9206, MI		•				
				9615, MI		•				
				9635M, I		•				
				9650, MI						
				3905, MS	•					
				3909W, I						
				3920, MS	•					
				3939, MS						
				3953, MS						
				3996AU,						
				ar, QCM						
			ŭ	.5, SC818	•	•				
				45, SDM						
				50, SDM	•	•				
				36, SDM	•	•				
				10, SDM	•	•				
				0, SDX24	•	•				
				50, SM7	150, SM	8150,				
			SM82	,		1 0046				
				dragon_H		d_2016				
			, SXRT	1130, SX	R2130					
			CVE I	D : CVE-	2019-2	271				
			Lack	of integri	ty checl	ζ	https:/	//ww		
			allow	s MODE	A to acco	ept any	w.qual	com		
Improper			NAS n	nessages	which o	can	m.com	/com	O-QUA-	APO8-
Authenticati	21-11-2019	10	result	into aut	henticat	tion	pany/	produ	031219	•
on			bypas	s of NAS	in	ct-			, - / -	
			Snapdragon Auto,					ty/bu		
			Snapdragon Compute,					/octo		
CV Scoring Scal	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)				121						

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Snapo Snapo Mobil Musio Wear, APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR6	dragon C dragon Indragon Id dragon Id dragon Id de, Snapdrables in A 017, APC 096AU, A 9150, MI 9635M, Id 9635M, Id 18936M, I	onsume ndustria oT, Snap ragon Vagon APQ800 Q8053, APQ809 DM9625 DM9625 DM9655 GM8909, SM8937, SM8940, SM8976, ASM8976,	r IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, 40, 6, M439, M632, M670, M850, 5,	ber-20 bulleti	19-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information land land land land land land land lan	mation d k of addi done or rs in SDI dragon C dragon C dragon C dragon In	isclosures rang the Sys code. in uto, ompute onnectivonsume	re due ge sDBG , vity, er IOT,	https://w.qualm.com pany/jct- securit lletins/ber-20 bulleti	/com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch.	NCIIP	C ID
			Snapo Infras Netwo APQ8 MDM <sup>1</sup> MSM8 MSM8 MSM8 QCS4 <sup>1</sup> SDA6 SDM6 SDM6 SDM6 SDM8	lragon_H	7ired and APQ80 Q8053, GM8905 M8917, M8953, cobar, Q 205, QM 345, SDM 450, SD 636, SD	09, , , , , , , , , , , , , , , , , , ,				
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer while stand user's Auto, Electric Snapo Snapo Snapo Infras Netwo APQ8 APQ8 IPQ40 MDM MDM MDM MSM8	Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and		https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	_	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297		
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8- 031219/294

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, SSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8- 031219/295
Out-of- bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in	https://ww w.qualcom m.com/com pany/produ	O-QUA-APQ8- 031219/296

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318	ct- security/bu lletins/octo ber-2019- bulletin	
mdm9207c_fi	rmware		Race condition due to the		
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, 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, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MDM9- 031219/297

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM632, SDM632, SDM632, SDM634, SDM636, SDM636, SDM50, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150   CVE ID: CVE-2019-10486	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free				MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150		
		21-11-2019	2.1	daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-	O-QUA- MDM9-

(CVSS)

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
Improper Validation of Array Index	21-11-2019	4.6	to imparray Auto, Electr Snape Snape Snape Snape APQ8 APQ8 APQ8 MDM MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8	occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503				//ww com /com produ ty/bu /octo 19- n	0-QUA- MDM9- 031219	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,				https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID				Pat	ch	NCIIP	C ID
			MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	9650, M3 3996AU, 174A, Q0 377, QC 605, QC 45, SDM 45, SDX 50, SM8	Nicobar CA6574, A9379, S405, Q0 670, SDI 20, SM6 250, SXI	CS605, M710, 150, R2130				
Use After Free	21-11-2019	4.6	CVE ID: CVE-2019-10566  Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150				https:/w.qual m.com pany/ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	/301
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,				https://w.qualm.com pany/jct- securitelletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/302
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID: CVE-2019-2268		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MDM9- 031219/303

2-3

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

Weakness	Publish Date	cvss	Description & CVE ID					ch	NCIIP	C ID
msm8905_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condition result in Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	process t messag tion is no cing into apdragon C dragon In dragon	re, Valid of met an infin in Auto, ompute onsume industria oT, Snap ragon Vagon APQ809 DM9607 DM9607 DM9605 SM8909, MSM891 SM8953, SM8	exit ite loop , er IOT, l IOT, dragon oice & e9, 8, 5, 7, 5, 40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150, d_2016	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/304
Time-of- check Time-	21-11-2019	4.4	Race condition due to the lack of resource lock which				https:/ w.qual	com	O-QUA- MSM8-	/O.O.T.
of-use			will be concurrently				m.com	/com	031219	/305
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ſ	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
(TOCTOU) Race Condition			statent bound Auto, Electr Snape Snape Snape Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81	fied in the nent lead access a Snapdra conics College Iragon Irag	ds to ou in Snape igon Cor onnectiv onsume idustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM893 Cobar, S405, Q0 60, SDA (439, SD (636, SD (636, SD	t of dragon asumer rity, er IOT, al IOT, odragon roice & 19, 18, 17, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18	pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo )19-		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM896AU, MSM898, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/307

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10503		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/308
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/309

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	[	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM9 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA84 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapd , SXR1	096AU, A 9150, MI 9206, MI 9635M, II 9635M, II 9635M, II 8905, MS 8909W, II 8920, MS 8939, MS 8939, MS 8953, MS 8920, MS	DM9205 DM9607 DM9625 MDM9645 SM8909, MSM891 SM8937, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDA 1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	98, CS605, A660, M439, M632, M670, M850, ,				
Improper Authenticati on	21-11-2019	10	allows NAS n result bypas Snape Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM9	of integrals MODEI nessages into aut s of NAS dragon A dragon C dragon In dragon Io e, Snapdo e, Snapdo ables in A 017, APO 096AU, A	M to accombined	ept any can tion  r IOT, l IOT, dragon oice & 9,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/310
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	CID
			MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	9615, MI 9635M, I 9635M, I 9650, MS 3905, MS 3909W, I 3939, MS 3953, MS 3953, MS 3996AU, ar, QCM 55, SDM 45, SDM 45, SDM 45, SDM 50, SDX24 50, SM7 50, SM7 50, SM7	MDM9655 M8909, MSM8916 MSM8940, MSM8976, MSM89 2150, Q 80X, SD 429, SD 1660, SD 1660, SD 1845, SD 150, SM High_Me R2130	40, 5, 17, 98, CS605, A660, M439, M670, M850, 5,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8998, Nicobar, QCS404,				https:/ w.qual m.com pany/ct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA- MSM8- 031219	/311
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	CVSS	Description & CVE ID			Pat	ch	NCIIP	C ID	
				SDA6 SDM6 SDM6 SDM6 SDM8 Snapo , SXR2	dragon_I	845, SDN 1450, SD 1636, SD 1710, SD High_Me	M429, M630, M660, M845, d_2016				
Integer Underflow (Wrap or Wraparound )	21	-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297				https://w.qualm.com/pany/jct-securitiletins/ber-20	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/312
Out-of- bounds Read	21	-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed				https:/ w.qual m.com pany/	lcom l/com	O-QUA- MSM8- 031219	/313
CV Scoring Scale (CVSS)	e	0-1	1-2	XID message. in Snapdragon  2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	Pat	ch	NCIIF	CID	
			Snapd Snapd Snapd Mobil- Music Weara APQ86 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA84 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapd , SXR1	Snapdra lragon Ic lragon Ic lragon Ic e, Snapdra bles in 2 017, APO 096AU, 2 9150, MI 9635M, Ic	onsume idustria of, Snap ragon Vagon APQ800 Q8053, APQ809 DM9625 MDM9655 MB9655 MB965 MB966, SM8940, SM8940, SM8940, SM8940, SM8940, SM8956, SD450, SD4660, SD46600, SD466000, SD4660000, SD4660000, SD4660000, SD46600000, SD46600000000000000000000000000000000000	r IOT, l IOT, dragon oice & 9, 8, 40, 7, 7, 7, 88, CS605, M439, M670, M850, , 8150,	ct- securit lletins ber-20 bulleti	octo 19-		
N/A	21-11-2019	7.2	copy for to the Param are from envirous Auto,	invoking from fd of secure lands because becau	or local bouffer, eing pop secure in Snapo gon Cor onnectiv	ouffer ulated dragon npute, vity,	https://w.qualm.com pany/jct- securit lletins ber-20	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	De	n & CVE	ID	Pat	ch	NCIIP	PC 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, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315				bulleti	n		
qcn7605_firm	ware									
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon				https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150  CVE ID: CVE-2019-10486		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM896AU, MSM8988, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCN7- 031219/316

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDX20 CVE ID : CVE-2019-10503		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20  CVE ID: CVE-2019-10535	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-QCN7- 031219/317
Out-of- bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-QCN7- 031219/318

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-QCN7- 031219/319
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing non- standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCN7- 031219/320

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297		
sdm845_firm	ware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8- 031219/321

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM4 SDM6 SDM6 SDM8 SDX5: SM81 Snapo	29, SDM 30, SDM 60, SDM 45, SDM 5, SM61 50, SM8 dragon_H	ligh_Me R2130	M450, M636, M710, X20, 150, d_2016				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130  CVE ID: CVE-2019-2339				https:/ w.qual m.com pany/j ct- securir lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon			https:/ w.qual m.com pany/s ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			Music Wears APQ8 APQ8 MDM' MDM' MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7	e, Snapdrables in A 017, APC 096AU, A 9206, MI 9607, MI 9650, MS 3909W, M 3953, MS 3998, Nic 605, QCS 29, SDM 4, SM615	ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8996, cobar, S405, Q0 6439, SD 636, SD	9, 8, 7C, 0, , 89, AU, CS605, 845, M630, M660, X20,				
Use After Free	21-11-2019	2.1	Use and daem static freed in Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MSM8 MSM8 MSM8	ter free free from shutd object in from a mapdragon Caragon Caragon Iragon Iragon, MS 9150, MS 9150, MS 937, MS 937, MS 937, MS 9340, MS	issue in lown du stance pultiple in Auto, ompute onnectivonsume on Vagon APQ800 Q8053, APQ809 QM9206 M8905 GM8905 GM8909 QM8939, GM8939, GM893	Xtra e to getting places  vity, r IOT, dragon oice &  9,  8, , , , , , , , , , , , , , , , ,	https:/w.qualm.com pany/ct- securilletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	:ch	NCIIP	C ID
			MSM8 SDA6 SDM6 SDM8 SM61 SM82	3996, MS 3998, Nio 60, SDAS 660, SDM 445, SDX 50, SM7 50, SXR2	cobar, Q 345, SDM 1670, SD 20, SDX 150, SM 2130	CS605, 4450, M710, 24, 8150,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8996AU, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- 031219	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch:	NCIIP	CID
			Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bi from a source that the potent buffer Snape Sna	tmap file any un-a e, there he bitma tially can roverflo dragon C dragon C dragon C dragon I dragon W 016, APC 098, MD 3996AU, ar, QCS4 55P, SC8 45, SDM 660, SDM 50, SM7 50, SM7 50, SXR2	e is load authenticis a possip can use stactive. In auto, ompute onnective onsume adustria flobile, foice & MQ8096A M9205, MSM89 405, QCS 180X, Single 1670, SD 1850, SD 150, SM 1130, SX 1130,	ed cated sibility k  vity, er city, er IOT, d IOT, Music in U, 98, 6605, DA660, M636, M710, X24, 8150, XR2130	https:/w.qualm.com pany/ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Use After	21-11-2019	4.6	Possible double free issue in			https:/	//ww	O-QUA-	SDM8-	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Free			camer modu Snapo Snapo Snapo Mobil Musio Wears Wired Netwo IPQ40 MDM0 MDM0 MSM8 QCA9	l while he a sensor les power lagon Aragon Infragon Infragon Infrastrocking in 19, IPQ8 19607, MS 1909W, MS 1909W, MS 1980, QCS 145, SDX 150	r and its er seque uto, onsume dustria oT, Snap ragon apdrago apdrago APQ80 3064, DM9207 SM8909 Vicobar, S405, Q0	ence in er IOT, el IOT, edragon oice & on and e53, e7C, e7C,	w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	031219	/328
			CVE I	D : CVE-	2019-2	266				
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA-3	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150		
			CVE ID : CVE-2019-2268		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9640, MDM9635M, MDM9645, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8937, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2271	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDM8- 031219/330
CV Scoring Scal					

(CVSS)

Authenticati on 21-11-2019 10 MDM9653, M, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8937, MSM8990, MSM8937, MSM8996, MSM8998, Nicobar, QCM2150, QC\$605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289  Improper Restriction of 21-11-2019 2.1 Information disclosure due to lack of address range check done on the SysDBG w.com/com m.com/com	Weakness	Publish Date	cvss	ſ	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Restriction of 21-11-2019 2.1 to lack of address range check done on the SysDBG m.com/com 0-QUA-SDM8-031219/332	Improper Authenticati on	21-11-2019	10	allows NAS n result bypas Snape Snape Snape Snape Snape Snape Snape Mobil Music Wear APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	s MODEN nessages into aut s of NAS lragon A lragon C lragon In lra	M to acc swhich of thentical in uto, ompute onsume industrial oT, Snap ragon V agon APQ800 Q8053, APQ809 DM9605 DM9625 DM9625 DM9625 DM9625 DM9635 SM8909, MSM891 SM8937, SM8940, SM8976, MSM891 SM891	ept any can tion  for IOT, al IOT, adragon foice & foi	w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	_	
of check done on the SysDBG m.com/com	Improper Restriction	21-11-2019	2.1	to lack of address range				w.qualcom			
		e 0-1	1-2	check 2-3	done on	the Sys	SDBG 5-6	m.com	/com 7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
Operations within the Bounds of a Memory Buffer			buffer Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 MDM <sup>6</sup> MSM8 MSM8 MSM8 MSM8 SDA6 SDM4 SDM6 SDM6 SDM6 SDM8 Snapo	rs in SDI dragon A dragon C dragon C dragon I dragon I dragon W dragon M dr	code. in auto, Compute Connective Consume Industria Mobile, Voice & Mobile Industria Mobile, Voice & Mobile Industria Mobile, Voice & Mobile Industria Mobile, SM8937,	yity, er IOT, el IOT, fusic, fusic, cS404, 215, M429, M630, M660, M845, d_2016	pany/yct-securit lletins ber-20 bulleti	ty/bu /octo )19-		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stands user's Auto, Electric Snape Snape Snape Snape Snape Snape APQ8	r overflo process ard NAN space. in Snapdra conics Co dragon C dragon W dragon W dragon W structure orking ir 017, APO	ing non- I messag Snapdra agon Cor onnectiv Consume ndustria Mobile, Voice & M Vired e and n APQ80 Q8053,	ge from agon sumer ity, er IOT, di IOT, Music,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM' MDM' MSM8 QCA6 QCA9 QCS40 SDA8 SDM8	019, IPQ 9206, M 9607, M 9650, M 3996AU, 574AU, 379, QC 05, QCS6 45, SDM 45, SDX 50	DM9207 DM964( SM8905 QCA617 QCA937 N7605, S05, SDA 636, SDA	7C, 7C, 74A, 77, 1660, M660, 24,				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modulout side it receive essage. Snapdra dragon Idragon Idra	its bounces malfin Snaper Gonsume and striate of the consumer	ndary ormed dragon mpute, er IOT, al IOT, odragon Voice & 19, 18, 5, 40, 5, 40, 5, 40, 5, 40, 5, 40, 5, 40, 5, 40, 60, M632,	https:/w.qualm.com pany/ct- securit lletins ber-20 bulleti	ty/bu /octo	O-QUA-9 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8953, MSM8996, MSM896AU, MSM8953, MSM8996, SDM630, SDM630, SDM632, SDM636, SDM630, SDM630, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8- 031219/335

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			, SXR1	130, SX	R2130					
			CVE I	D : CVE-	2019-2	315				
Use After Free	21-11-2019	7.2	cleand missing for a fapplic Comp Consu Indus Mobil Infras Netwo QCS40 SDM6 SDX55 SM81	ter free up routing points ailed station. in ute, Snaute, Snaute, Snapd tructure orking in 04, QCS6, SM61, SM61, SM61, SM61, SM61, SXR	ne due to er sanitiz ort of a tr Snapdr pdragon C, Snapdr C, Snapdr ragon W e and MDM92 605, SDA 6710, SD 50, SM71	rusted agon ragon ragon ragon 845, 845, 845, R2130	https:/ w.qual m.com pany/ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9 031219	
apq8017_firm	1ware		CVET	D. CVE-	2017-2.	<i>,</i>				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
			MSM8	•	SM8909,	•				

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130						
			CVE I	D : CVE-	2019-2	335				
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modified stater bound Auto, Electric Snape Mobil Music Wears APQ8 APQ8 MDM MDM MDM MSM8 MSM8 MSM8 MSM8 QCN7	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, 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, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845,				//ww lcom n/com produ ty/bu /octo 019- n	0-QUA- 031219	•
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150		
			CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130  CVE ID: CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8- 031219/339
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://ww w.qualcom m.com/com pany/produ ct- security/bu	0-QUA-APQ8- 031219/340
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM <sup>o</sup> MSM8 MSM8 MSM8 MSM8 MSM8	lragon C lragon In lragon V lragon V lragon W 009, APO 053, APO 098, MD 9207C, M 9640, MS 3905, MS 3905, MS 3905, MS 3905, MS 3905, SDA 30, SDM	ndustria lobile, oice & M /earable (8017, (8096A M9206, MDM960 (M8909, MSM893, MSM8933, MSM8933,	I IOT,  Music, es in  U,  77, 7, 17, 18, 198, 0M450,	lletins ber-20 bulleti	19-		
			Buffer		w can o	ccur in				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	rates elements and control of the co	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605,				//ww .com ./com produ ty/bu /octo 119- n	O-QUA 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130		
			CVE ID : CVE-2019-10566		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150  CVE ID: CVE-2019-2268	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-APQ8- 031219/342
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-APQ8- 031219/343
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> SDM <sup>o</sup> SDA <sup>o</sup> SDM <sup>o</sup> SD	096AU, A 9150, MI 9206, MI 9615, MI 9635M, II 9635M, II 89650, MS 8905, MS 8909W, II 8920, MS 8939, MS 8953, MS 8953, MS 8953, MS 8050, SDM 10, SDM 1130, SM 1130, SX 1130, SX 1130, SX 1130, SX	DM9205 DM9607 DM9625 MDM9645 SM8909, MSM891 SM8937, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDA 1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	98, CS605, A660, M439, M632, M670, M850, ,				
Improper Authenticati on	21-11-2019	10	allown NAS named Snaped Snaped Snaped Snaped Mobil Musica Weard APQ8 APQ8 MDM	of integrals MODER nessages into autoris of NAS dragon A dragon C dragon In dragon In dragon In 2, Snapdr 2, Snapdr 2, Snapdr 3017, APO 9150, MI 9206, MI	M to accombined	ept any can tion  r IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR2	9615, Mi 9635M, I 9650, Mi 8905, Ms 8909W, I 8920, Ms 8939, Ms 8953, Ms 8953, Ms 8953, Ms 896AU, bar, QCM 150, SDM 150, SDM 10, SDM 10, SDM 10, SDM 10, SDM 110, SM7 1130, SX D: CVE-	MDM96-55 M8909, MSM891 SM8940, SM8940, SM8976, MSM89 2150, Qu 80X, SDA 429, SDI 1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	98, CS605, A660, M439, M670, M850, ,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape Snape Snape Snape Snape Snape Snape Snape Snape Month MSM8 MSM8 MSM8	mation d k of addi done or s in SDI dragon C dragon C dragon C dragon W dragon W dragon W dragon W dragon W STUCTURE 017, APO 9205, MS 8909, MS	ress range the System the System to the Syst	ge DBG vity, r IOT, l IOT, fusic,	https:/w.qualm.com pany/jct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publi	ish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
				SDA6 SDM6 SDM6 SDM6 SDM8 Snapo	lragon_I	345, SDN 1450, SD 1636, SD 1710, SD High_Me	M429, M630, M660, M845, d_2016				
Integer Underflow (Wrap or Wraparound )	21-1	1-2019	4.6	while stand user's Auto, Electric Snape Snape Snape Infras Network APQ8 APQ8 IPQ40 MDM MDM MDM MDM MSM8 QCA6 QCS4 SDA8 SDM8 SM81	r overfloor process and NAN space. in Snapdra conics Coloragon Maragon Maragon Warructure orking in 017, APO 064, APO 019, IPQ 9206, Maragon M	ing non- I message Snapdra agon Cor connective consume ndustria Mobile, Vired e and n APQ80 Q8053, Q8096A 8064, IP DM9640 SM8905 QCA617 QCA937 N7605, 605, SDA 636, SDA	ge from agon sumer ity, er IOT, l IOT	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com orodu cy/bu /octo 19-	0-QUA- 031219	•
Out-of- bounds Read	21-1	1-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon				https:/ w.qual m.com pany/	com /com	0-QUA- 031219	•
CV Scoring Scale (CVSS)	e	0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pat	ch	NCIII	PC ID
			Snapd Snapd Snapd Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA84 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapd	Snapdra lragon Ic lragon Ic lragon Ic e, Snapdra bles in 2 017, APC 096AU, 2 9150, MI 9635M, Ic	onsume industria of, Snap lragon V ragon APQ800 Q8053, APQ809 DM9625 DM9655 GM8909, MSM891 GM8976, MSM8976, SDM5630, SDM660, SDM6429, SDM6430, SDM64300,	r IOT, l IOT, dragon oice & 9, 8, 40, 5, 7, 7, 28, CS605, M439, M670, M632, M670, M850, ,	ct- securit lletins, ber-20 bulleti	octo 19-		
N/A	21-11-2019	7.2	copy for to the Param are from envirous Auto,	invoking from fd of secure lands because becau	or local buffer, eing pop secure in Snapo gon Condonnectiv	ouffer oulated dragon npute, vity,	https://w.qual m.com pany/j ct- securit lletins/ ber-20	com /com orodu cy/bu /octo	0-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo Infras Netwo APQ8 APQ8 APQ8 MDM' MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SM81 Snapo	dragon Indragon Wilragon Wilragon Wilragon Wilragon Wilragon Wilragon, APO 1098, MD 1096, APO 1098,	Mobile, Foice & Mobile, Foice	Music,  09,  U,  98,  215,  M429,  M630,  M660,  M845,  7150,  d_2016	bulleti	n		
Out-of- bounds Read	21-11-2019	2.1	Trust memo result Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo	decure Ko zone to o ory read into DO dragon A dragon C dragon I dragon V dragon V dragon V dragon V orking in 053, APO	do an ari which w S in uto, onnectiv onsume ndustria fobile, foice & M Vired and APQ80 Q8096,	bitrary vill vity, r IOT, l IOT, fusic,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318		
apq8096au_fi	irmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8- 031219/350

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Time-of-check Time-of-use (TOCTOU) Race Condition	Publish Date  21-11-2019	4.4	SDX5. SM81 Snapo , SXR1 CVE I Race of lack of will be modified states and the states are shown of the	5, SM61: 50, SM8 dragon_H 130, SX D: CVE- conditio f resour e concur fied in the nent lead d access Snapdra onics Co dragon I dragon I dragon I dragon I e, Snapdra shles in 017, AP 9206, M 9607, M 9650, M 9650, M	50, SM7 250, High_Me R2130 2019-2 In due to ce lock verently le memoration Snapel agon Corronnective consume in Snapel agon Corronnective consume APQ800 Q8053, APQ809 DM9640 SM8905 MSM893	the which spy t of dragon sumer ity, old IOT, odragon foice & 19, 8, 7C, 19, 19, 19, 19, 19, 19, 19, 19, 19, 19	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	//ww lcom l/com produ ty/bu /octo	O-QUA- 031219	APQ8-
			MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX2 SM81	3953, MS 3998, Ni 605, QC 5, SDA6 29, SDM 32, SDM 10, SDM	5M8996. cobar, S405, Q0 60, SDA 1439, SD 1636, SD 1845, SD 50, SM7	AU, CS605, 845, M630, M660, X20,				
Use After Free	21-11-2019	2.1	Use at daem static freed	fter free on shuto object in from a r	issue in lown du nstance ; nultiple	Xtra e to getting	https:/ w.qual m.com pany/	lcom l/com	0-QUA- 031219	-
			in Snapdragon Auto,				ct-			
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6				6-7	7-8	7-8 8-9 9-	

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SM61 SM82		connections consumerations and a strict consumerations. Since the consumeration of the consum	vity, or IOT, ol IOT, odragon oice & 9, 8, 5, 77, , W, CS605, M450, M710, 24, 8150,	securit lletins ber-20 bulleti	octo 19-		
Improper Validation of Array Index	21-11-2019	4.6	CVE ID: CVE-2019-10490  Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearable, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,				https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			MSM8 MSM8 MSM8 QCN7 SDM6 SDX2		MSM8937, 5M8937, 5M8953, MSM89 A660, SI	98, 0M450, M660,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improvarial firmwhound function through Auto, Snapo Snapo Snapo Snapo APQ8 APQ8 MSM8 QCA6 QCS44 SDM8	per valiole receivare can di accession while gh loop Snapdradragon Conics Colragon In dragon Maragon Wolfagon W	dation for ved from lead to do in WLAI en iteration in Snaper Consumer on sume	or loop n out of N ng dragon npute, or ity, or IOT, I IOT, U, 98, 5, 845,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	lcom n/com produ ty/bu /octo	0-QUA- 031219	-
Out-of- bounds Read	21-11-2019	4.6	in fast to imp while from Snapo Snapo Electr Snapo Snapo	r over-re t messag proper in process firmwar dragon A dragon C dragon I dragon M	ge handlenput val ing a me e in auto, onsume onnective onsume	er due idation essage r ity, r IOT,	https://w.qualm.com/pany/ct-securilletinsber-20	lcom n/com produ ty/bu /octo	0-QUA 031219	-
CV Scoring Scal	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 MSM8 QCN7 SDA6	lragon V 053, AP( 3996AU, 605, QC 60, SDM 0, SDX24	Q8096A MSM89 S405, Q0 636, SDI	U, 98, CS605,				
			CVE I	D : CVE-	2019-1	0563				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	wlandrates elements than in Snapor Snapor Snapor Snapor Snapor Snapor APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	r overflomodule for extendent length max rate dragon Aragon Concist College of the control of th	if suppoded rate his greaten set lenguto, compute on sume on nective donsume on dustria Mobile, Momento Moment	rted es eter eth in r ity, r IOT, l IOT, fusic in 06, 07, , 7, AU, CS605, M710, 150, R2130	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	-
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute,				https://w.qualm.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	0-QUA 031219	•
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	bulletin	
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-APQ8- 031219/358

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			CVE I	D : CVE-	2019-2	268				
Out-of- bounds Read	21-11-2019	10	while session messarun-in Snapo Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 MDM MDM MDM MDM MDM MSM3 MSM3 MSM3 MSM3	r over reparsing on manages if no tended with the design of the design o	downlingement etwork stalues in auto, compute consume industria oT, Snap dragon Wagon APQ800 DM9625 DM9625 DM9625 DM9625 DM9625 DM9625 DM9655	nk OTA sends , er IOT, dl IOT, dragon oice & 19, 40, 5, 17, , 17, , 18, 18, 18, 198, CS605, A660, M439, M632, M632, M670, M850, 5, 8150, d_2016	https:/w.qualm.com pany/ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
Improper	21-11-2019	10	Lack of integrity check			https:/	//ww	O-QUA-	APQ8-	
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	[	Description	n & CVE	ID	Pat	ch	NCIII	PC ID
Authenticati			allows	s MODE	I to acc	ept any	w.qual	com	031219	9/360
on			NAS n	nessages	which	can	m.com	/com		
			result	into aut	hentica	tion	pany/j	produ		
			bypas	s of NAS	in		ct-			
			_	lragon A			securit	ty/bu		
			Snapd	lragon C	ompute	,	lletins			
			^	lragon C			ber-20			
			_	lragon Ir			bulleti	n		
			_	lragon Io	•	•				
				e, Snapd	•	oice &				
				, Snapdr	•	_				
				ables in A	•	9,				
			_	017, AP(	•	_				
			_	096AU, A	_					
				9150, MI						
				9206, MI						
			MDM							
				9635M, I		•				
				9650, MI		•				
				8905, MS	•					
				8909W, N		•				
				8920, MS						
				8939, MS 8953, MS						
				8996AU,						
				ar, QCM		•				
				5, SC818		•				
			~	3, 30010 45, SDM	•	•				
				50, SDM	•	•				
				36, SDM	•	•				
				10, SDM	•	•				
				10, 3DM ), SDX24	•	•				
				50, SM7:	•	•				
			SM82		150, 5141	0150,				
				lragon_H	ligh Me	d 2016				
				.130, SX		u_2010				
				D : CVE-		289				
Integer				overflo			https://	/ /\\\		
Underflow				process			https://ww w.qualcom		O-QUA-	-APQ8-
(Wrap or	21-11-2019	4.6		messag		-		031219	-	
Wraparound				Snapdra		pany/j	•		,	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Electr Snapo Snapo Snapo Snapo Infras Netwo APQ8 IPQ40 MDM' MDM' MDM' MDM' MSM8 QCA6 QCA9 QCS40 SDA8 SDM8 SM81	Snapdra conics Co dragon C dragon M dragon W dragon W dragon W dragon W dragon W dragon W 017, APC 064, APC 019, IPQS 9206, MI 9650, MS 379, QCI 379, QCI	onnective onsume adustria flobile, foice & M Vired and APQ80 Q8053, Q8096Al B064, IP DM9640 SM8905, QCA617 QCA937 N7605, SO5, SDA 636, SDI 20, SDX2	ity, r IOT, l IOT, lusic,  09, U, Q8074, C, , 74A, 77, 660,	ct- securit lletins ber-20 bulleti	octo 19-		
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM	P modulout side it receives age. it sage. it sage it s	its bour res malfo in Snapo agon Con onsume ndustria oT, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9605	ndary ormed lragon npute, r IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch:	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	3905, MS 3909W, MS 3920, MS 3939, MS 3953, MS 3996AU, ar, QCMS 45, SC818 45, SDM 450, SDM 50, SDX24 50, SM7 50, dragon_H	MSM8917, SM8940, SM8976, MSM89 2150, Quantum 20, SD 429, SD 429, SD 6660, SD 6660, SD 6845, SD 50, SM High_Me	98, CS605, A660, M439, M632, M670, M850,				
			CVE I	D : CVE-	2019-2	303				
N/A	21-11-2019	7.2	copy to the Param are from environment of Snapo	e invokin from fd of secure landers be om non soment. Snapdradragon Calragon Calragon Maragon Waragon Waragon Waragon Waragon Waragon Waructure 017, APC 096, APC 098, MD 9205, MI 9607, MI 3905, MS 3917, MS	or local laboration of local laborations of laborations o	ouffer oulated dragon npute, vity, r IOT, l IOT, fusic, 09,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 QCS46 SDA6 SDM6 SDM6 SDM8 SM81 Snapo	3953, MS 3996AU, 04, QCS6 60, SDA6 33, SDM 32, SDM 50, SM6 50, SM6 50, dragon_F 1130, SX <b>D: CVE</b> -	MSM89 505, QM 345, SDN 1450, SD 1636, SD 1710, SD 150, SM High_Me R2130	98, 215, M429, M630, M660, M845, 7150, d_2016				
Out-of- bounds Read	21-11-2019	2.1	Trust memore result Snapo Snap	decure Kory read into DO dragon Adragon Coloragon Williagon Willia	do an ar which was in auto, connectionsume adustrial fobile, foice & Marian Wired and APQ80 28096, IPQ8074 SM8920, SM8940, QCA808 429, SDM	bitrary vill vity, or IOT, l IOT, lusic, 17, 4, 4, 181, 1439, d_2016	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
msm8976_fir	mware									
Loop with Unreachable Exit Condition	21-11-2019	5	Reject condi	process t messag tion is na ing into	ge, Valid ot met	exit	https://w.qual m.com pany/j	com /com	0-QUA- MSM8- 031219	/365
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Descriptio	on & CVE	ID	Pat	ch	NCIIF	PC ID
('Infinite Loop')			Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SC818 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SDX58 SM81 Snapo , SXR1	apdragon C dragon C dragon Indragon Indragon Ic dragon Ic dragon Ic e, Snapdrables in A 017, APC 096AU, A 9150, MI 9615, MI 9635M, I 9635M, I 9635M, I 9635M, I 9635M, I 9635M, I 9630, MS 3998, Nic 2150, QC 30X, SDA 29, SDM 30X, SDA 429, SDM 50, SDM 50, SDM 51, SM615 50, SM615 1130, SXI	ompute, onsume adustria oT, Snap dragon Vagon APQ800 Q8053, APQ809 DM9605 DM9605 DM9605 DM9605 DM8909, MSM8916 GM8937, SM8953,	r IOT, dragon foice & 9, 8, 5, 7, 40, 5, 40, 6, M215, M450, M636, M710, X20, 150, d_2016	ct- securit lletins, ber-20 bulleti	octo 19-		
Out-of- bounds Read	21-11-2019	10	while session messa un-int Snapo Snapo Snapo	r over re parsing on manag ages if ne tended v dragon A dragon C dragon I	downlir gement ( etwork s ralues in uto, ompute, onsume	nk OTA eends r IOT,	https://w.qualm.com pany/jct- securit lletins/ ber-20	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	l	Description	on & CVE	Pat	ch	NCIIP	C ID	
			Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	dragon lo e, Snapdo c, Snapdo doles in 2 017, APO 096AU, 2 9150, Mi 9615, Mi 9635M, Mi 9635M, Mi 9635M, Mi 9635M, Mi 9635M, Mi 9635M, Mi 9909W, I 8909W, I 890W, I 890W, I 890W, I 890W, I 890W, I 890W, I 890W, I	Iragon V ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MDM9655 SM8909, MSM8937, SM8940, SM8976, MSM89 2150, Qu 80X, SDA 429, SDA 1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	Foice & 9, 8, 5, 7, 5, 40, 5, 4660, M439, M632, M670, M850, 5, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	bulleti	n		
Improper Authenticati on	21-11-2019	10	allows NAS n result bypas Snapo Snapo Snapo Snapo Snapo Snapo Mobil	of integros MODEl nessages into aut res of NAS dragon A dragon C dragon I dragon I dragon I dragon I dragon I dragon I dragon I dragon I	M to acc s which of thentica S in Sompute Sonsume ndustria oT, Snap Iragon V	ept any can tion , er IOT, l IOT, dragon	https://w.qualm.com pany/jct- securitelletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/367
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	ables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 3905, MS 3905, MS 3905, MS 3996AU, 45, SC818 45, SC818 45, SDM 45, SDM 710, SDM 710, SDM 0, SDX24 50, SM7	APQ800 Q8053, APQ809 DM9607 DM9605 DM9655 MB909, MSM8916, SM8937, SM8940, SM8937, SM8940, SM8937, SM8940, SM8937, SM8955 SM8956, MSM89 EMBERT SD SM8955 SM8976, MSM89 SM8955 SM8976, MSM89 SM8937, SM8	9, 8, 5, 40, 5, 40, 6, 7, 68, 6805, 6860, 6832, 6870, 68150, 62016				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM	P modulout side it receives sage. It sages that the sages in the sages	its bour res malfo in Snapo agon Cor onsume ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809	ndary ormed dragon npute, r IOT, dragon oice & 9,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303		
sda845_firmv	vare				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDA8- 031219/369

Weakness	Publish Date	cvss	1	Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9650, M. 3905, M. 3905, M. 3920, M. 3940, M. 3976, M. 3998, Nic. 2150, QC 300, SDM 45, SDM 5, SM61. 50, SM8 dragon_H 1130, SX D: CVE-	5M8909, MSM8937, 5M8953, 5M8996, cobar, S605, Q 1632, SD 1632, SD 1670, SD 1850, SD 50, SM7 250, High_Me R2130	M215, A845, M450, M636, M710, X20, 150, d_2016				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out o lack of array image Snapo Snap	f bound of check of size white elf segn Adragon Adragon Chagon Indragon Maragon Witructure orking in 104, QCS6 150, SDM 150, SM7 130, SXR D: CVE-	access definition of while reading the reading terms of the computer of the co	ue to elist ng the , vity, er IOT, l IOT, 205, 845, M845, 55,	https:/w.qualm.com pany/ct- securilletins ber-20	lcom l/com produ ty/bu /octo	0-QUA- 031219	
Time-of- check Time- of-use	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently				https://ww w.qualcom m.com/com		0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Descriptio	on & CVE	ID	Pat	ch	NCIIP	C ID
(TOCTOU) Race Condition			stater bound Auto, Electr Snape Snape Snape Mobil Music Wears APQ8 MDM' MDM' MDM' MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81	fied in the nent lead access in Snapdra fonics Colleagon Ir dragon	ds to out in Snape in Snape gon Cor onnectiv onsume ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905 MSM805	t of dragon asumer ity, r IOT, l IOT, dragon foice & 9, 8, 7C, 9, 89, AU, CS605, 845, M630, M660, X20, 150,	pany/j ct- securit lletins, ber-20 bulleti	ty/bu /octo )19-		
Use After Free	21-11-2019	2.1	daem static freed in Sna Snapo Snapo Snapo Snapo Mobil Music Wears	fter free and shutded object in from a mager of the strage	lown dunstance gondtiple had Auto, compute, consume hadustria bT, Snap lragon Vagon	e to getting places  vity, r IOT, l IOT, dragon oice &	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pul	blish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
				MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61 SM82	096AU, 2 9150, M 9207C, M 9650, M 8909, M 8917, M 8937, M 8937, M 8996, M 8996, M 60, SDM 660, SDM 660, SDM 50, SM7 50, SXR2	DM9206 MDM960 SM8905 SM8909 SM8939, SM8953, SM8956, SOBAT, Q B45, SDM 1670, SD 20, SDX 150, SM	5, 07, , , W, AU, CS605, M450, M710, 24,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-	-11-2019	2.1	varial firmw bound functi throu Auto, Snapo Snapo Snapo APQ8 APQ8 MSM8 QCA6 QCS4 SDM8	oper valioner valione	ved from lead to of in WLAI e iteration in Snapo agon Consume consume consume donume industria Mobile, Moice & M Q8096A MSM89 QCN760 605, SDA 20	nout of N ng dragon mpute, r ity, r IOT, l IOT, U, 98, 5,	https:/w.qualm.company/jct-securitelletins/ber-20	com /com produ ty/bu /octo	0-QUA- 031219	
Buffer Copy without				Buffer overflow can occur in wlan module if supported				https:/ w.qual	•	O-QUA-	SDA8-
Checking Size of Input	21-	-11-2019	4.6	rates or extended rates element length is greater			m.com	/com	031219		
CV Scoring Scale (CVSS)	e	0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	Pat	ch	NCIIP	CID	
('Classic Buffer Overflow')			Snapo Snapo Snapo Snapo Snapo Snapo Snapo APQ8 MDM9 MDM9 MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	max rate dragon A dragon C dragon C dragon I dragon W dragon W 017, APO 096AU, I 9207C, M 9650, M	auto, compute consume consume consume dobile, coice & M Q8053, MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0 670, SD0 20, SM6	ity, ity, ity, ity, I IOT, I IOT, Music in 06, 07, , , XI, XI, XI, XI, XI, XI, XI, XI, XI	ct- securit lletins ber-20 bulleti	/octo )19-		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from a source that the potent buffer Snape	tmap file any un-a e, there he bitma tially car roverflo dragon A dragon C	is a possip can use stack w. in auto, compute consume on sume on sume on sume foice & March 1986 (Soice & March 1986), QCS	cated cibility k  vity, cr ity, cr IOT, l IOT, l U, 98, 605,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-3	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

SDA845, SDM636, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130   CVE ID: CVE-2019-2251   Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Compute, Snapdragon Compute, Snapdragon IoT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8096, MDM9205, MDM9205, MDM9205, MDM9205, MDM9206, MDM9635, MDM9635, MDM9635, MDM9635, MSM8909, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8933, MSM8940, MSM8933, MSM8940, MSM8933, MSM8940, MSM8933, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM215, CQC805, QM215, SC8180X, SDM630, SDM632, SDM630, SDM632, SDM636, SDM645, SDM850, SDX20, SDX20, SDX24, SDX55, SDX24, SDX55, SDX20, SDX24, SDX55,	Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM96030, SDM8980, Nicobar, QCM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM630, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,				SDM6 SDM8 SM61 SM82	560, SDM 345, SDM 50, SM7 50, SXR	1670, SD 1850, SD 150, SM 1130, SX	M710, X24, 8150, R2130				
SM6150, SM7150, SM8150, SM8250,		21-11-2019	10	while session messar un-in Snapo Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	parsing on manage ages if no tended with t	downlingement (etwork straines in auto, compute of consume ndustria of the con	nk OTA ends r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, 47, 40, 6, 40, 6, M439, M632, M670, M850,	w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	=	
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1	_	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130		
			CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9625, MDM9635M, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8953, SDM630, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8- 031219/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130  CVE ID: CVE-2019-2295	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDA8- 031219/378
			Buffer overflow can occur	https://ww	
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while processing non- standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDA8- 031219/379

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS	l	Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			Infras Netwo APQ8 APQ8 IPQ40 MDM <sup>o</sup> MDM <sup>o</sup> MSM8 QCA6 QCA9 QCS40 SDA8	dragon V structure orking ir 017, APO 064, APO 019, IPQO 9607, MI 9650, MI 379, QCI 05, QCSO 45, SDM 645, SDX	e and n APQ80 Q8053, Q8096A B064, IP DM9207 DM9640 SM8905 QCA617 QCA937 N7605, S05, SDA	U, Q8074, CC, ), 74A, 7, .660, M660,				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear; APQ8 APQ8 MDM' MDM' MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8	D: CVE-P modul out side it receive tessage. Snapdradragon Indragon	e may active bounders malformands trian bound by the boun	ccess ndary ormed dragon npute, r IOT, l IOT, dragon oice & 9, 8, 6, 7, 1, 40, 6, 1, 17,	https:/w.qualm.com pany/jct- securifiletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA-9	
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)										

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			QM21 SDA8- SDM6 SDM7 SDX2- SM61 SM82 Snapo	ar, QCM 5, SC818 45, SDM 36, SDM 10, SDM 0, SDX24 50, SM7 50, dragon_H 130, SX <b>D: CVE-</b>	30X, SDA 429, SDA 630, SD 660, SD 845, SD 7, SDX55 150, SM High_Me R2130	A660, M439, M632, M670, M850, , 8150, d_2016				
N/A	21-11-2019	7.2	copy for the Paramare from the	invoking from fd of secure lands on secure lan	or local lands of local lands of local lands of local lands of lands of local lan	ouffer oulated dragon npute, vity, r IOT, l IOT, U, 09, U, 5, 0,	https:/w.qualm.com pany/ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-3 031219	
			SDM4	60, SDA8 39, SDM 32, SDM		M630,				

Weakness	Publish Date	cvss	l	Description	on & CVE I	D	Pat	ch	NCIIP	C ID
			SDM8 SM81 Snapo , SXR1	50, SM6 50, lragon_F .130, SX	1710, SDI 150, SM' High_Med R2130 <b>2019-2</b> 3	7150, l_2016				
Use After Free	21-11-2019	7.2	cleand missing for a fapplic Comp Consu Indus Mobil Infras Netwo QCS40 SDM6 SDX55 SM81	ng pointo ailed sta ation. in ute, Sna mer IOT trial IOT e, Snapd tructure orking in 04, QCS6 70, SDM 5, SM615	ne due to er sanitiz art of a tr Snapdragon T, Snapdragon We and MDM92 505, SDAS 1710, SDI 50, SM71	cation usted agon ragon agon fired 205, 845, M845, 50, R2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
sdm636_firm	ware									
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,		https:/ w.qual m.com pany/j ct- securit lletins, ber-20	com /com produ ty/bu /octo	0-QUA- 031219			
			APQ8 MDM9 MDM9	096AU, A 9150, MI 9206, MI	Q8053, APQ8098	•	bulleti	n		

Weakness	Publish Date	cvss	1	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9635M, 9650, M 8905, M 8909W, M 8920, M 8940, M 8976, M 8998, Ni 645, SDM 660, SDM 645, SDM 5, SM61 50, SM8 dragon_H	DM9655 SM8909, MSM8937, SM8953, SM8996, Cobar, S605, Q M660, SD M632, SD M670, SD M850, SD M850, SM7	M215, M215, M450, M636, M710, X20,				
			CVE I	D : CVE-	2019-2	335				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modified stater bound Auto, Electric Snape Mobil Music Wear APQ8 APQ8 MDM MDM MDM MSM8 MSM8	condition of resour econcurried in the ment lead access Snapdragon Idragon Idr	ce lock werently the memory in Snaper in Snaper ingon Corr consumer industria oT, Snaper lragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905	which rpy t of dragon nsumer ity, or IOT, dragon foice & re g, 8, 7C, 0, , 39,	https:/ w.qual m.com pany/s ct- securing lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-: 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	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, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID: CVE-2019-10486		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8940, MSM8953, MSM896AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDM6- 031219/385
Out-of- bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo	O-QUA-SDM6- 031219/386
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pul	blish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
				Snapo Snapo Snapo APQ8 MSM8 QCN7 SDA6 SDX2	onics Co dragon D dragon M dragon V 053, APO 8996AU, 605, QCO 60, SDM 0, SDX24	onsume ndustria lobile, loice & M Q8096A MSM89 S405, Q0 636, SDI	Tr IOT, I IOT, Music in U, 98, CS605, M660,	ber-20 bulleti			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-	11-2019	7.2	If a bi from source that to potent buffer Snape	tmap file any un-a e, there he bitma tially ca roverflo dragon C dragon C dragon C dragon C dragon W dragon W 016, APO 098, MD 8996AU, ar, QCS4 55P, SC8 45, SDM 660, SDM 645, SDM 50, SM7 50, SM7	e is loade authentic is a possip can use stack w. in auto, compute connective consume adustria dobile, coice & MO (28096A) MSM89 (405, QCS) (4670, SD) (46	ed cated sibility k  vity, or ity, l IOT, l	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com orodu cy/bu /octo 19-	O-QUA- 031219	
Out-of- bounds Read	21-	11-2019	7.5	P2P a	ole 00B ction fra ing WLA	mes wh		rur annalaam		0-QUA- 031219	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	[	Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			Snaped Snaped Snaped Snaped Snaped Snaped APQ8 APQ8 APQ8 MDM9 MDM9 MSM8 QCA6 QCA9 SDA66 SDM6	gement for the second s	uto, onsume onnectiv onsume ndustria lobile, oice & N Q8017, Q8096A M9206, MDM960 SM8996 A6174A QCA937 S405, QO 630, SDI 670, SD	er ity, er IOT, l IOT, Music in U, O7, AU, A, 7, CS605, M636, M710, 150	pany/j ct- securii lletins ber-20 bulleti	ty/bu /octo )19-		
Out-of- bounds Read	21-11-2019	10	Buffer while session messar un-interest Snaped Snaped Snaped Snaped Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM	c over reparsing on manages if netended valragon Caragon Caragon Iragon Iragon, MI 19635, MI 19635, MI 19635, MI 19650, MI 19650, MI 19650, MI 19650, MI	ad can had can	nappen nk OTA sends or IOT, ol IOT, odragon oice & o o o o o o o o o o o o o o o o o o o	https:/ w.qual m.com pany/j ct- securif lletins ber-20 bulleti	ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX2 SM61 SM82 Snapo	3909W, I 3920, MS 3939, MS 3953, MS 3996AU, ar, QCM 55, SC818 45, SDM 50, SDM 710, SDM 710, SDM 750, SM7 50, dragon_H 1130, SX	5M8937, 5M8940, 5M8976, MSM89 2150, Q0 30X, SDA 429, SDI 6630, SD 6660, SD 845, SD 845, SD 150, SM	98, CS605, A660, M439, M632, M670, M850, ,,				
Improper Authenticati on	21-11-2019	10	Lack of allow NAS result bypas Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MSM8 MSM8	of integris MODEN nessages into aut is of NAS dragon A dragon C dragon In dragon Ic dragon Ic dragon Ic e, Snapdr ables in A 9150, MI 9206, MI 9635M, I 9635M, I 9635M, I 89630, MS	ity check M to accombined to chentical in uto, ompute onsume ot, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9625 MDM9645 SM8909, MSM891	ept any can tion  r IOT, l IOT, dragon oice &  9,  8,  7,  40,  5,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			MSM8 Nicob QM21 SDA8- SDM4 SDM7 SDX20 SM61 SM82 Snapo	3953, MS 3996AU, ar, QCM 5, SC818 45, SDM 50, SDM 10, SDM 0, SDX24 50, SM7 50, SM7 1130, SX D: CVE-	MSM89 2150, Q 80X, SDA 429, SDI 1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	98, CS605, A660, M439, M632, M670, M850, 5, 8150,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape Sna	mation dak of addition of addition of addition of addition of agon of	ress range the System the System to the Syst	ge sDBG vity, vity, r IOT, l IOT, Music, 09, , , CS404, 215, M429, M630, M660, M845,	https:/w.qualm.com pany/ct-securi lletins ber-20 bulleti	ty/bu /octo	0-QUA-9 031219	
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1		-	<b>J</b> 7	. 3	- 5 6	<b>,</b>	, , ,		3 10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Integer Underflow (Wrap or Wraparound	Publish Date  21-11-2019	4.6	Ruffer while stand user stand user stand user stand user stand user stand stand stand stand Snape Snap	•	2019-2  ow can o ing non- ing non- imessage Snapdra agon Cor onnective consume ndustria dobile, voice & M Vired e and n APQ80 Q8053, Q8096A 8064, IP DM9207 DM9640 SM8905 QCA617 QCA937 N7605, 605, SDA	295 ccur ge from agon asumer ity, ar IOT, I IOT, I IOT, Q8074, 7C, 0, 74A, 77, 4660, M660,	https:/w.qualm.company/jct-securitelletins.ber-20	//ww com /com produ ty/bu /octo	O-QUA- 031219	SDM6-
			SM81							
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MI 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3953, MS 3953, MS 3953, MS 36, SDM 45, SDM 45, SDM 50, SDX24 50, SM7 50, SM7	Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 GM8909, MSM8916, GM8976, MSM8976, MSM89, Q150, Q0 80X, SDA 429, SDI 8630, SDA 1660, SD 1845, SD 150, SM High_Me R2130	8, 5, 6, 40, 6, 40, 5, 7, 25, 27, 4660, M439, M670, M632, M670, M850,				
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
sdm670_firm	ware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6- 031219/395

Weakness	Publish Date	cvss	1	Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDX5 SM81 Snapo	3909W, 1 3920, MS 3940, MS 3976, MS 3998, Nio 2150, QC 30X, SDM 30X, SDM 30	5M8937, 5M8953, 5M8996, cobar, S605, Q 1660, SD 1632, SD 1670, SD 1670, SD 1850, SM7 250, High_Me R2130	M215, A845, M450, M636, M710, X20, 150,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	lack of array image Snape Snap	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130				//ww lcom n/com produ ty/bu /octo )19- n	0-QUA- 031219	
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto,			https:/ w.qual m.com pany/j	lcom 1/com	0-QUA- 031219		
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	2-3 3-4 4-5 5-6		6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM8	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130				ty/bu /octo 119- n		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	cvss	Description & CVE ID				Pat	ch	NCIIP	CID
				MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81 CVE I	9650, M 3996AU, 174A, Q 377, QC 605, QC 45, SDM 845, SDX 50, SM8 <b>D : CVE</b> -	Nicobar CA6574 A9379, S405, Q0 670, SDI 20, SM6 250, SXI	CS605, M710, 150, R2130				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-	-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID: CVE-2019-2251				https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA- 031219	
Out-of- bounds Read	21	-11-2019	7.5	Possible 00B read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto,			https://w.qual m.com pany/j	com /com	0-QUA-SDM6- 031219/400		
CV Scoring Scal (CVSS)	е	0-1	1-2	2-3	-3 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	Pat	ch.	NCIIP	C ID	
			Electr Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 SDA6 SDM6	dragon Conics Co	onnectivonsume ndustria Jobile, Joice & M Q8017, Q8096A M9206, MDM960 SM8996 A6174A QCA937 S405, QO	ity, or IOT, l IOT, fusic in U, O7, AU, A, 7, CS605, M636, M710,	securion lletins ber-20 bulleti	/octo )19-		
			CVE I	D : CVE-	2019-2	268				
Out-of- bounds Read	21-11-2019	10	while session messar un-information of Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8	r over reparsing manages if netended valended va	downlingement of tworks alues in uto, ompute onsume ndustria oT, Snapragon Vagon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9655 MB9695 MSM891	nk OTA sends  r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5,	https:/ w.qual m.com pany/j ct- securing lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX20 SM61 SM82 Snapo	3939, MS 3953, MS 3996AU, ar, QCM 5, SC818 45, SDM 36, SDM 10, SDM 50, SDX24 50, SM7 50, dragon_H	5M8976, MSM89 2150, Q0 80X, SDA 429, SDI 6630, SD 6660, SD 845, SD 150, SM High_Me R2130	98, CS605, A660, M439, M632, M670, M850, 5, 8150,				
Improper Authenticati on	21-11-2019	10	Lack of allow. NAS in result bypas Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integriss MODEN nessages into aut is of NAS dragon A dragon C dragon Ic d	ity check M to accombined to chentical in auto, ompute onsume adustria oT, Snap ragon APQ800 Q8053, APQ809 DM9205 DM9625 DM9625 MDM9625 MDM9625 MDM9645 SM8909, MSM8916, SM8940, SM8940,	ept any can tion  r IOT, l IOT, dragon oice &  9,  8, 5, 40, 5,	https:/w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-3 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	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, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, SDM630, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDM6- 031219/403

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2295		
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2303	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6- 031219/404
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer,	https://ww w.qualcom m.com/com	0-QUA-SDM6- 031219/405

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	[	Description	n & CVE	ID	Pat	ch	NCIII	PC ID
Weakiress			Paramare from environment of the	neters becoment. Snapdradragon Clragon Irlagon Maragon Williagon Williagon, Milliagon, Milliago	eing pope secure in Snape igon Cor onnectivonsume industria lobile, foice & Maria Vired and APQ80 (28053, Q8096A (28096A) (28096A	oulated dragon inpute, vity, r IOT, l	pany/j ct- securit lletins ber-20 bulleti	produ ty/bu /octo 119-	NCIII .	
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired				https://w.qualm.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID: CVE-2019-2329	bulletin	
sdm710_firm	ware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7- 031219/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130		
			CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130  CVE ID: CVE-2019-2339	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDM7- 031219/408
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-SDM7- 031219/409
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	ľ	Descriptio	n & CVE	ID	Pat	ch	NCIIP	CID
			MDM <sup>4</sup> MSM <sup>8</sup> MSM <sup>8</sup> QCN <sup>7</sup> QM21 SDM <sup>4</sup> SDM <sup>6</sup> SDM <sup>7</sup> SDX2 <sup>4</sup> SM81	9607, MI 9650, MS 3909W, M 3953, MS 3998, Nic 605, QCS 5, SDA6 29, SDM 32, SDM 10, SDM 4, SM615 50	5M8905 MSM8936 SM8996 Cobar, 5405, QO 60, SDA 4439, SD 636, SD 845, SD	, 39, AU, CS605, 845, M630, M660, X20,				
Use After Free	21-11-2019	2.1	Use and daemond static freed in Snape Snape Snape Snape Snape Snape Snape Snape Mobil Music Wears APQ8 MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 SDA66 SDM6 SDM8	fter free and shutdon	issue in lown du stance gon lown dustria on sume industria oT, Snap ragon Vagon APQ800 Q8053, APQ809 DM9206 GM8905	Xtra e to getting places  vity, r IOT, l IOT, dragon oice &  9,  8,  7,  W,  AU, CS605, M450, M710, 24,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9 031219	
CV Scoring Scal			214101	JU, JIVI / .	100,0141	0100,				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130		
<u> </u>			CVE ID : CVE-2019-10490		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7- 031219/411
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDM7- 031219/412
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch:	NCIIP	C ID
			Snapo APQ8 APQ8 MSM8 Nicob SA61! SDA8 SDM6 SDM8 SM61 SM82	dragon M dragon V 016, APO 098, MD 3996AU, ar, QCS4 55P, SC8 45, SDM 660, SDM 50, SM7 50, SXR2	Toice & M Q8096A M9205, MSM89 405, QCS 180X, SD 1670, SD 1670, SD 1850, SM 1130, SX	U, 98, 605, DA660, M636, M710, X24, 8150,				
Out-of- bounds Read	21-11-2019	7.5	P2P a handl mana Snapo Snapo Snapo Snapo APQ8 APQ8 MDM MSM8 QCA6 QCA9 SDA6 SDM8	ole OOB ction fra ing WLA gement dragon A dragon C dragon I dragon I dragon V 009, AP 053, AP 098, MD 9207C, M 9650, M 379, QC 574AU, 1 379, QC 60, SDM 660, SDM 645, SDX D: CVE-	imes whan Inframe in Luto, Ionsume Ionsume Ionsume Ionsume Iobile, Ioce & M Q8017, Q8096A IOM960 SM8996 CA6174A QCA937 S405, QC 630, SDI 1670, SD 20, SM6	ile ir ity, ity, I IOT, I IOT, Ausic in U, 7, AU, A, 7, CS605, M636, M710, 150	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Out-of- bounds Read	21-11-2019	10	while sessic	r over re parsing on mana ages if ne	downlir gement (	nk OTA	https://ww w.qualcom m.com/com pany/produ		v.qualcom 0-QUA-SDM7 n.com/com 031219/414	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	Pat	ch	NCIIF	PC ID	
			un-in	tended v	alues in		ct-			
			Snapo	dragon A	uto,		securi	ty/bu		
			Snapo	dragon C	ompute	,	lletins	octo/		
			^	dragon C			ber-20			
			^	dragon Ir			bulleti	n		
			Snapo	dragon Io	T, Snap	dragon				
			Mobil	e, Snapd	ragon V	oice &				
				:, Snapdr	_					
				ables in A	_	9,				
			_	017, AP0	•					
			_	096AU,	•					
				9150, MI						
				9206, MI		•				
				9615, MI		•				
				9635M, I						
				9650, MI						
				3905, MS	•					
				3909W, I						
				3920, MS	•					
				3939, MS						
				3953, MS						
				3996AU,						
				ar, QCM						
			·	.5, SC818	•	•				
				45, SDM						
				50, SDM	•	•				
				36, SDM	•	•				
				'10, SDM	•	•				
				0, SDX24	•	•				
				50, SM7	150, SM	8150,				
			SM82	-	r. l. M.	1 2016				
				dragon_H		a_2016				
				1130, SX						
			CVE I	D : CVE-	2019-2	271				
			Lack	of integri	ity checl	ζ	https:/	//ww		
 				s MODE			w.qual	com		
Improper		4.5		nessages			m.com	/com	O-QUA-	SDM7-
Authenticati	21-11-2019	10		into aut		tion	pany/j	produ	031219	
on			bypass of NAS in							•
			Snapdragon Auto,					ty/bu		
			Snapdragon Compute,					/octo		
CV Scoring Scal	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)				221						

Weakness	Publish Date	cvss		Description	on & CVE	Pat	ch:	NCIIF	PC ID	
			Snapo Snapo Snapo Mobil Musio Wear: APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	dragon C dragon In dragon Id e, Snapdr ables in A 017, APC 096AU, A 9150, MI 9635M, I 9635M, I 9635M, I 9635M, I 3905, MS 3905, SDM 450, SDM	onsume adustria oT, Snap Iragon Vagon APQ800 Q8053, APQ809 DM9625 MDM9625 MDM9655 MB9676, MSM8937, SM8940, SM8976, MSM8940, SDA 429, SDA 4	r IOT, l IOT, dragon oice & 9, 8, 40, 5, 40, 5, 40, 5, 40, 6, M439, M632, M670, M850, , 8150,	ber-20 bulleti			
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snapo Snapo Snapo Snapo Snapo	mation d k of addi done or dragon A dragon C dragon C dragon C dragon I	ress rang the Sys code. in outo, ompute onnectiv onsume ndustria	ge DBG , vity, r IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	O-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	tch	NCIIP	C ID
			Snapo Infras Netwo APQ8 MDM' MSM8 MSM8 MSM8 QCS40 SDA6 SDM6 SDM6 SDM6	lragon_H	7ired and APQ80 Q8053, GM8905 M8917, M8953, cobar, Q 05, QM 345, SD 450, SD 636, SD 710, SD	09, , , , 215, , , , , , , , , , , , , , , , , , ,				
			CVE I	D : CVE-	2019-2	295				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8	P modul out side it receiv lessage, i Snapdra dragon Ir dragon Ir dragon Ir dragon Ir dragon Ir 2017, APC 096AU, A 9150, MI 9615, MI 9635M, I 9635M, I 9630, MI 3905, MS	its bour es malfo in Snapo gon Cor onsume ndustria oT, Snap ragon V agon APQ800 Q8053, APQ809 DM9605 DM9625 MDM964 DM9655 MB909, MSM891	ndary ormed dragon npute, r IOT, l IOT, dragon foice &  9,  8, 5, 7, 6, 40, 6,	https:/ w.qual m.com pany/j ct- securi lletins ber-20 bulleti	lcom n/com produ ty/bu /octo 019-	0-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 Nicob QM21 SDA8- SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	3953, MS 3996AU, ar, QCM 5, SC818 45, SDM 50, SDM 10, SDM 50, SM7 50, SM7 1ragon_H 1130, SXI	MSM89 2150, Q 30X, SDA 429, SDA 630, SD 660, SD 845, SD 5, SDX55 150, SM ligh_Me R2130	98, CS605, A660, M439, M632, M670, M850, ,				
N/A	21-11-2019	7.2	copy for the the Paramare from	e invoking from fd of secure be neters be om non soment. Snapdradragon Chragon Chragon Maragon Working in 017, APC 098, MD 9205, MI 8905, MS 8937,	or local lands of loc	ouffer oulated dragon npute, vity, r IOT, l IOT, U, 09, U, 5, 0, 98,	https://w.qualm.com pany/jct- securitelletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-3 031219	
CV Scoring Scale	e 0-1	1-2	2-3		<u> </u>	-	<u> </u>	7-8	8-9	

Weakness	Publish Date	cvss	l	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDM6 SDM8 SM81 Snapo	39, SDM 32, SDM 70, SDM 50, SM6 50, dragon_H 130, SX <b>D: CVE-</b>	1636, SD 1710, SD 150, SM High_Me R2130	M660, M845, 7150, d_2016				
Use After Free	21-11-2019	7.2	cleand missing for a fapplic Comp Consu Indus Mobil Infras Netwo QCS40 SDM6 SDX55 SM81	ter free up routing points ailed state ation. in ute, Snaumer IOT trial IOT e, Snapd tructure orking ir 04, QCS6, SM61, SM61, SM61, SXR2 D: CVE-	ne due to er saniti art of a tr Snapdr pdragon T, Snapdr T, Snapdr Tagon W E and MDM9 505, SDA 1710, SD 50, SM7	rusted ragon ragon Vired 205, 845, M845, 150, R2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9	
sm6150_firm	ware									
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi result in Sna Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8	t message tion is no ing into apdragon dragon C dragon I dragon I	te, Valid ot met an infin n Auto, ompute onsume ndustria oT, Snap ragon V ragon APQ800 Q8053, APQ809	exit ite loop r IOT, l IOT, dragon oice &	https://w.qualm.com pany//ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-3	
CV Scoring Scal			2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch:	NCIIF	C ID
			MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> SC818 SC818 SDM <sup>o</sup> SDX5 <sup>o</sup> SM81 Snapo , SXR1		DM9625 MDM9655 MSM8909 MSM8937 SM8953 SM8956 Cobar, S605, Q 1632, SD 1632, SD 1670, SD	M215, M215, M450, M636, M710, M20, M2016				
Use After Free	21-11-2019	4.9	CVE ID: CVE-2019-2335  Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130  CVE ID: CVE-2019-2336				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Improper Restriction	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist				https:/ w.qual		0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
of Operations within the Bounds of a Memory Buffer			image Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo QCS40 SDM6 SDM6 SM61	size which elf segration Alragon Coloragon Indragon Waragon Waragon Waragon Waragon Waructure 194, QCS 6, SDX 150, SDX 130, SXR	nents. in auto, compute connection consume ndustria Mobile, Vired e and n MDM9 605, SDA 1710, SD 24, SDX 150, SM	, vity, er IOT, l IOT, 205, 845, M845,	m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race of lack of will be modified stater bound Auto, Electron Snape Mobil Music Wears APQ8 APQ8 MDM MDM MDM MSM8 MSM8 MSM8 MSM8 QCN7	condition of resource concurring in the nent lead access Snapdra conics Colleagon Idragon Idra	n due to ce lock we rently de memo ds to out in Snapo agon Cor onsume ndustria oT, Snap lragon V ragon APQ809 DM9207 DM9640 SM8905 MSM893 cobar, S405, Q0	the which apy tof dragon asumer ity, adragon foice & 9, 8, 7C, 9, 89, AU, CS605,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-9 031219	
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pul	blish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
				SDM6 SDM7	29, SDM 32, SDM 10, SDM 4, SM61!	1636, SD 1845, SD	M660, X20,				
				CVE I	D : CVE-	2019-1	0486				
Use After Free	21-	11-2019	2.1	daem static freed in Sna Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musio Wear APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61 SM82	fter free on shutch object in from a map dragon of drago	lown dunstance in Auto, and auto, and auto, and auto, and auto auto auto auto auto auto auto auto	e to getting places , vity, er IOT, l IOT, dragon oice & 9, 8, 5, 77, , W, CS605, M450, M710, 24, 8150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Buffer Copy					r overflo			https:/	•	O-QUA-	SM61-
without Checking	21-	11-2019	4.6	rates	module : or exten	ded rate	es	w.qual m.com	/com	031219	
Size of Input				element length is greater				pany/	produ		
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
('Classic Buffer Overflow')			Snapo Snapo Snapo Snapo Snapo Snapo Snapo APQ8 MDM' MDM' MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	max rate dragon A dragon C dragon C dragon In dragon I dragon V 017, APO 096AU, I 9207C, M 9650, MS 377, QCA 605, QCS 45, SDM 645, SDM 50, SMS	ompute onsume onnectivonsume onsume o	or ity, or IOT, of IOT, dusic in 06, 07, , CS605, M710, 150, R2130	ct- securii lletins ber-20 bulleti	octo )19-		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bi from a source that the potent buffer Snape Sna	tmap file any un-a e, there i he bitma tially cau dragon A dragon C dragon C dragon C dragon C dragon M dragon W 016, APC 098, MD 3996AU, par, QCS4	e is load uthentics a possup can use stactive onnective onsume on	ed cated sibility k  vity, er ity, l IOT, l IOT, U, 98,	https:/ w.qual m.com pany/j ct- securif lletins ber-20 bulleti	ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDM8 SM61 SM82 CVE I	45, SDM 60, SDM 45, SDM 50, SM7 50, SXR:	1670, SD 1850, SD 150, SM 1130, SX <b>2019-2</b>	M710, X24, 8150, (R2130				
Out-of- bounds Read	21-11-2019	7.5	P2P a handl mana, Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 MDM MSM8 QCA6 QCA9 SDA6 SDM6 SDM8	ole OOB ction fra ing WLA gement i dragon A dragon C dragon C dragon M dragon M dragon W 009, AP 0098, MD 0207C, M 098, MD 0207C, M 098, QC 0574AU, 0 0574AU	imes whan frame in fr	ile  er ity, er IOT, l IOT, Music in U, A, 7, CS605, M636, M710, 150	https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &				https://w.qualm.com pany/jct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	c, Snapdrables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MS 3905, MS 3909W, I 3920, MS 3939, MS 3939, MS 3953, MS 3	APQ800 Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 GM8909, MSM8937, GM8940, SM8976, MSM8976, MSM89, E300, SD 429, SD 429, SD 429, SD 429, SD 4429, S	18, 5, 7, 5, 40, 5, 17, 198, CS605, A660, M439, M632, M670, M850, 5, 8150, d_2016				
Improper Authenticati on	21-11-2019	10	allowan NAS m result bypas Snapo Snapo Snapo Snapo Mobil Music Weara	of integriss MODEN nessages into aut is of NAS dragon A dragon C dragon I dragon I dragon I c, Snapdr ables in A	M to acc s which thentica s in outo, ompute onsume ndustria oT, Snap dragon V ragon	ept any can tion er IOT, al IOT, odragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> SDM <sup>o</sup> SDA <sup>o</sup> SDM <sup>o</sup> SD	096AU, A 9150, MI 9206, MI 9615, MI 9635M, II 9635M, II 8905, MS 8905, MS 8920, MS 8939, MS 8953, MS 8953, MS 8953, MS 805, SDM 15, SC818 16, SDM 10, SDM 10, SDM 10, SDM 10, SDM 10, SDM 1130, SM 1130, SX 1130, SX 1130, SX 1130, SX	DM9205 DM9607 DM9625 MDM9655 MSM8909, MSM8937, SM8940, SM8976, MSM89 2150, Qu 80X, SDA 429, SDA 1630, SDA 1630, SDA 150, SM High_Me R2130	5, 7, 6, 40, 6, 40, 7, 7, 27, 28, 28, 28, 46, 46, 46, 46, 46, 46, 46, 46, 46, 46				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Mobil Music Weara APQ8 APQ8 MDM MDM MDM	P modulout side it receives sage. Snapdradragon Indragon	its bounders malfoling Snapon Coronsume andustria porto T, Snapon Varagon Varagon Varagon Q8053, APQ809 DM9205 DM9607 DM9625	ndary ormed dragon npute, r IOT, l IOT, dragon oice &  9,  8, 6, 7,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	tch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	9650, MI 3905, MS 3909W, NS 3920, MS 3939, MS 3953, MS 3996AU, ar, QCM 55, SC818 45, SDM 450, SDM 710, SDM 710, SDM 50, SM7 50, dragon_H	M8909, MSM891 M8940, M8976, MSM89 2150, Qe 30X, SD 429, SDI 630, SD 660, SD 845, SD 5, SDX55 150, SM	98, CS605, A660, M439, M632, M670, M850,				
				<b>D : CVE-</b>						
N/A	21-11-2019	7.2	copy to the Paramare frenvire Auto, Snape	from fd of secure lands on non sonment. Snapdra dragon Caragon Maragon Waragon Waragon Waragon Waructure orking in 017, APC 098, MD 9205, MD 9607,	or local bouffer, eing popsecure in Snapegon Coronsumendustria dobile, oice & Marcolo (28053, 28096A) (28096A)	ouffer oulated dragon npute, vity, r IOT, l IOT, dusic, 09, U,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	l l	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 QCS46 SDA66 SDM6 SDM6 SDM8 SM81 Snapo	3937, MS 3953, MS 3996AU, 04, QCS6 60, SDA6 39, SDM 570, SDM 550, SM6 50, dragon_H 130, SX <b>D: CVE-</b>	5M8996, MSM89 505, QM 345, SDM 1450, SD 1636, SD 1710, SD 150, SM High_Me R2130	98, 215, 4429, M630, M660, M845, 7150,				
Use After Free	21-11-2019	7.2	cleand missing for a fapplic Comp Consu Indus Mobil Infras Netwo QCS40 SDM6 SDX55 SM81	tter free up routing point failed station. in the cation i	ne due to er saniti ort of a to Snapdr pdragor F, Snapdr Iragon V e and on MDM9 605, SDA 1710, SD 50, SM7	zation rusted ragon ragon vired 205, 845, M845, 150,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-: 031219	
qm215_firmw	vare									
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &				https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-031219	-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch:	NCIIP	CID
			Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SDM4 SDM6 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo , SXR1	c, Snapdrables in A 017, APC 096AU, A 9150, MI 9206, MI 9635M, I 9635M, I 9635M, I 3905, MS 3909W, I 3976, MS 3976, MS 3976, MS 3976, MS 3976, MS 3976, MS 3976, MS 3976, SDM 50, SDM 50, SDM 5150, SDM 545, SDM	APQ800 Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 GM8909, MSM891 GM8953, GM895	8, 5, 7, 6, 40, 5, 40, 17, AU, M215, A845, M450, M636, M710, X20, 150, d_2016				
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modified stater bound Auto, Electron Snapo Snapo Mobil Music Wears	condition of resource e concur fied in the ment lead d access Snapdra conics Co dragon Indragon Indrag	ce lock verently e memods to our in Snape gon Cor onnective onsume ndustria oT, Snape ragon Veragon APQ800	which  Try  t of  dragon  issumer  ity,  or IOT,  dragon  oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>o</sup> MDM <sup>o</sup> MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7	096AU, A 9206, MI 9607, MI 9650, MS 3909W, N 3953, MS 3998, Nic 605, QCS 5, SDA6 429, SDM 410, SDM 4, SM615	DM9207 DM9640 SM8905 MSM893 SM8996 Cobar, S405, Q0 60, SDA (439, SD (636, SD	CC, ), , 39, AU, CS605, 845, M630, M660, X20,				
			CVE I	D : CVE-	2019-1	0486				
Out-of- bounds Read	21-11-2019	10	while session messar un-interpretation of the session messar un-interpretation of the session of	r over reparsing on manages if netended volvagen Caragon Caragon Interpretation (Caragon Interpretation) (Caragon Interpr	downlingement (extwork straines in uto, ompute onsume ndustria oT, Snaperagon Vagon APQ800 Q8053, APQ809 DM9625 DM9625 DM9625 DM9625 DM9625 DM9655 GM8909, MSM8917, GM8940, GM8976, GM	nk OTA sends  r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5,	https:/ w.qual m.com pany/j ct- securif lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-031219	-
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			QM21 SDA8 SDM6 SDM7 SDX2 SM61 SM82 Snapo	ar, QCM .5, SC81; 45, SDM .50, SDM .10, SDM .10, SDM .50, SM7 .50, SM7 .1130, SX D: CVE-	80X, SDA 429, SDA 1630, SDA 1660, SDA 1845, SDA 150, SMA High_Me R2130	A660, M439, M632, M670, M850, 8150, d_2016				
Improper Authenticati on	21-11-2019	10	Lack of allow NAS in result bypas Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integrals MODEl nessages into autorises of NAS dragon Adragon Adragon Idragon Idrag	ity check M to access which a chentical in auto, compute consume andustrial oT, Snap dragon V ragon APQ800 Q8053, APQ809 DM9607 DM9607 DM9607 DM9607 DM9607 SM8909, MSM891 SM8937, SM8940, SM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976,	k ept any can tion  r IOT, dragon oice &  8,  17,  17,  18,  17,  17,  18,  17,  18,  19,  19,  10,  10,  10,  10,  11,  11,  12,  13,  140,  15,  16,  17,  18,  18,  18,  18,  18,  19	https:/w.qualm.company/jct-securitelins.ber-20	com /com produ ty/bu /octo	0-QUA-0 031219	-
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR2	lragon_H 1130, SX <b>D : CVE-</b>	660, SD 845, SD 5, SDX55 150, SM High_Me R2130 <b>2019-2</b>	M670, M850, 8150, d_2016				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lace check buffer Snape SNAS	dragon_F	ress range the System to code. in the System to, ompute onnection on sume adustrial folice & March 1980 (1980) (19	ge sDBG , vity, er IOT, l IOT, Music, 09, , , , , , , , , , , , , , , , , ,	https://w.qualm.com/pany/jct-securityletins/ber-20	com /com produ ty/bu /octo	0-QUA- 031219	-
Out-of- bounds Read	21-11-2019	7.5		P modul	-		https:/	•	0-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	out side	4-5	5-6	w.qual	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
Weakness	Publish Date	CVSS	when XID mand Auto, Snaped Snaped Snaped Snaped Mobil Music Wears APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	it receives tessage. It is received to the sage of the	res malforin Snaporagon Consume adustria of T, Snaporagon Veragon APQ800 Q8053, APQ809 DM9607 DM9625 MB9607 DM9655 GM8909, MSM891 GM8940, GM8940, GM8976, MSM89 Q2150, Q01660, SD G845,	ormed dragon inpute, in IOT, dragon oice & 9, 8, 5, 40, 7, 7, 15605, 1660, 166	n.com pany/j ct- securit lletins, ber-20 bulleti	/com produ ty/bu /octo 19- n	NCIIP	PC ID
N/A	21-11-2019	7.2	Parameters being populated are from non secure environment. in Snapdragon					/com produ ty/bu /octo	0-QUA- 031219	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIF	CID
			Snapo Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 APQ8 APQ8 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SM81 Snapo	lragon C lragon I lragon I lragon V lragon V lragon V tructure orking in 017, APC 098, MD 9205, MI 9607, MI 8905, MS 8917, MS 8937, MS 8937, MS 8953, MS	onnective onsume adustria flobile, foice & Movired and a APQ80 (APQ80)	vity, r IOT, l IOT, lusic,  09,  U,  98, 215, 4429, M630, M660, M845, 7150, d_2016	ber-20 bulleti	19-		
Out-of- bounds Read	21-11-2019	2.1	Trustomemo result Snapo Snapo Snapo Snapo Snapo Snapo Snapo Infras	ecure Kezone to cory read into DO dragon Chragon Maragon Waragon Waragon Waragon Waragon Waragon Waragon Waragon Waragon Waructure	do an ar' which w S in uto, onnectiv onsume ndustria fobile, foice & M Vired	bitrary vill vity, r IOT, l IOT, Iusic,	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish	n Date	cvss		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
				APQ8 MSM8 MSM8 MSM8 QM21 SDM4 Snapo	8053, AP 8096AU, 8917, MS 8937, MS 8953, MS 8996AU, 15, SDM 450, SDM dragon_F	IPQ8074 SM8920 SM8940 SM8996 QCA808 429, SDN 1632, High_Me	31, 1439, d_2016				
qca8081_firm	iware										
Out-of- bounds Read	21-11-	-2019	2.1	Trust memore result Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo Infras Netw APQ8 APQ8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 Snapo	Secure Korzone to o cory read tinto DC dragon A dragon C dragon I dragon V dragon V dragon V structure orking in 8053, AP 8937, MS 8937, MS 8937, MS 8937, MS 8937, MS 8953, MS 8953, MS 6096AU, 15, SDM dragon_I dragon_I dragon_I dragon_I dragon_I dragon_I dragon_I	do an ar which which which wells in auto, consume adustria dobile, which we and a APQ80 Q8096, IPQ8074 GM8940,	bitrary vill vity, or IOT, l IOT, l IOT, 4, 4, 6, 117, 4439, 64_2016	https:/ w.qua m.com pany/ ct- securi lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- 031219	-
qcs404_firmv	vare										
Use After Free	21-11-	-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in						0-QUA- 031219	•
CV Scoring Scal (CVSS)	le 0	)-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[	Descriptio	n & CVE	ID	Pat	ch	NCIII	PC ID
			Snapd Snapd Snapd Snapd Snapd Snapd Infras Netwo QCS40 SM71	lragon A lragon Ca lragon Ca lragon Ir lragon W lragon W tructure orking in 04, SDX5 50, SM82	ompute onnection onsume ndustria lobile, loice & M Vired and and MDM9 55, SM61	vity, er IOT, ll IOT, Music, 205, 150, R2130	ct- securit lletins, ber-20 bulleti	octo 19-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	lack o array image Snapd	f bound a f check of size whith elf segnal lragon Callagon Callagon In lragon In lragon In lragon Watructure orking in 04, QCS6 70, SDM 50, SDX2 50, SM72 130, SXR	of whilted le readinents. in uto, omputed onsumed industriation on MDM9 in MDM	elist ng the  , vity, er IOT, l IOT, 205, 845, M845, 55,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	•
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snapd Snapd Snapd	nation d c of addr done on rs in SDI Iragon A Iragon C Iragon C	ress rang the Sys code. in uto, ompute onnectiv	ge sDBG , , vity,	https://w.qual m.com pany/j ct- securit lletins/ ber-20	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			Snapo Snapo Snapo Infras Netwo APQ8 MDM <sup>6</sup> MSM8 MSM8 MSM8 QCS40 SDA6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8	lragon_H	Tobile, Toice & Marie And Toice & Marie And To APQ80 To A	Music, 09, , CS404, 215, M429, M630, M660, M845, d_2016	bulleti	n		
N/A	21-11-2019	7.2	copy for the the Param are from	e invoking from fd of secure lands on non soment. Snapdra dragon Caragon Maragon Waructure orking in 017, APO 1996, MD 19205, MD 19205, MD 19607,	or local louffer, eing popsecure in Snapelegon Coronsumendustria dobile, foice & Marcele and APQ80 (28053, Q8096A M9150, DM9206	ouffer oulated dragon mpute, vity, or IOT, I IOT, Uusic, U,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	1	Description	on & CVE	ID	Pat	ch	NCIIP	CID
			MSM8 MSM8 MSM8 QCS4 SDA6 SDM6 SDM6 SDM6 SDM8 SM81 Snapo	3905, MS 3917, MS 3937, MS 3953, MS 3996AU, 04, QCS6 60, SDM 632, SDM 670, SDM 570, SM6 50, dragon_H 1130, SX <b>D: CVE-</b>	5M8920, 5M8940, 5M8996, MSM89 505, QM2 845, SDM 1450, SD 1710, SD 150, SM High_Me R2130	98, 215, M429, M630, M660, M845, 7150,				
Use After Free	21-11-2019	7.2	cleand missing for a far application Compound Industrial Mobil Infrastrial Netwood QCS4 SDM6 SDX5 SM81	ter free up routing point failed station. ir oute, Snaumer IOT trial IOT e, Snape orking in 04, QCS6 570, SDM 5, SM61 50, SXR D: CVE-	ne due to er saniti art of a to a Snapdr pdragon T, Snapdo Iragon W e and a MDM9 605, SDA 1710, SD 50, SM7 1130, SX	zation rusted ragon ragon Vired 205, 845, M845, 150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
sm8150_firm	ware									
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi result in Sna Snapo Snapo	e process t messag tion is n ting into apdragon dragon C dragon C dragon I	ge, Valid ot met an infin n Auto, compute consume	exit ite loop , er IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIF	CID
			Snapo Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SC818 SDM6 SDM6 SDM6 SDM6 SDM8 SDX58 SM81 Snapo , SXR1	lragon Ide, Snapdrables in A 017, APC 096AU, A 9150, MI 9635M, I 9635M, I 8905, MS 8940, MS 8940, MS 8940, MS 8940, MS 8940, MS 895, SDA 29, SDA 29, SDA 29, SDA 29, SDA 29, SDA 20, S	DT, Snap ragon V ragon APQ800 Q8053, APQ809 DM9607 DM9625 MDM9655 MSM8937, GM8937, GM8953, SM8	dragon oice & 9, 8, 5, 40, 5, 40, 40, 40, 40, 40, 40, 40, 40, 40, 40	bulleti			
Use After Free	21-11-2019	4.9	listen memo use af Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo	quent user may repry corructer free in the largen Caragon Caragon Maragon Waragon Waragon Waragon Waragon Waragon Waragon Waragon Waructure	esult in option do issue. in uto, ompute onnectivo onsume ndustria dobile, oice & Mared	further ue to , vity, r IOT, l IOT,	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID: CVE-2019-2336		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130  CVE ID: CVE-2019-2339	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-SM81- 031219/449
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Woice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-SM81- 031219/450
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>6</sup> MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX2 SM81	9607, M3 9650, M3 3909W, I 3953, M3 3998, Nio 605, QC3 5, SDA6 29, SDM 32, SDM 4, SM615 50 <b>D: CVE</b> -	SM8905 MSM893 SM8996, cobar, S405, Q0 60, SDA (439, SD (636, SD (845, SD	, 39, AU, CS605, 845, M630, M660, X20,				
Use After Free	21-11-2019	2.1	Use and daem static freed in Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 MSM8	fter free on shutdon shutdon and pdragon Colragon Colragon Colragon Indicates in Augusta 19207C, March 19207C, Mar	issue in lown dunstance in Auto, ompute onnection on Sume industria of The Summer of T	Xtra e to getting places  vity, r IOT, l IOT, dragon oice &  9,  8,  7,  W,  AU, CS605, M450, M710, 24,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-9 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	Pat	ch	NCIIP	CID	
				50, SXR2 <b>D : CVE</b> -		0490				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	wlan rates elementhan in Snapo	r overflomodule or extendent length max rate dragon Adragon Conics Collragon Maragon M	if suppo ded rate h is grea set leng auto, compute consume onnectiv consume dobile, voice & M Q8053, MDM92 MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0 670, SD 20, SM6 250, SXI	rted es ater eth in  r ity, er IOT, l IOT,  Music in  06, 07, , 7, AU, CS605, M710, 150, R2130	https:/ w.qual m.com pany/ct- securif lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from source that the potent buffer Snape S	tmap filo any un-a e, there he bitma tially ca roverflo dragon A dragon C dragon C dragon C dragon C	is a possip can use stackw. in auto, compute consume c	cated sibility k , vity, er ity, er IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID: CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150  CVE ID: CVE-2019-2266	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SM81- 031219/454
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto,	https://ww w.qualcom m.com/com pany/produ ct- security/bu	O-QUA-SM81- 031219/455
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIII	PC ID
			Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musio Wears APQ8 MDMS MDMS MDMS MSM8 MSM8 MSM8 MSM8 MSM	dragon C dragon In dragon In dragon In dragon Io e, Snapdr ables in I 017, APO 096AU, I 9615, MI 9615, MI 9635M, I 9650, MI 3905, MS 3905, MS 3005, SDM 450, SDM	ompute, onsume adustria oT, Snap dragon Vagon APQ800 DM9607 DM9605 DM89076, DM80076, DM80076, DM80076, DM80076, DM80076, SD40076 DM96076, SD40076 DM96076, SD40076 DM96076 DM	r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, M439, M632, M670, M850, ,	lletins ber-20 bulleti	19-		
Improper Authenticati on	21-11-2019	10	allow NAS result bypas Snapo Snapo Snapo	of integr s MODEl nessages into aut ss of NAS dragon A dragon C dragon C	M to accommodate which of the conticate of the conticate of the continuation of the co	ept any can tion , r IOT,	https://w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIF	CID
			Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM4 SDM6 SDM7 SDM7 SDX20 SM61 SM82 Snapo , SXR1	dragon Ide, Snapdre, Snapdre, Snapdre, Snapdre, 2017, APC 206, MI 20650, MI 205, MI 205, SDM	lragon V ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MSM8937, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDI 1630, SD 1660, SD 1845, SD 150, SM	oice & 9, 8, 5, 7, 6, 40, 5, 4660, M439, M632, M670, M850, 6, 7, 8150, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	bulleti	n		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electric Snapo Snapo Snapo Snapo Snapo Snapo Snapo	r overflo process ard NAN space. in Snapdra conics Co dragon C dragon M dragon W dragon W	ing non- I messag Snapdra Igon Cor Ionsume Industria Iobile, Ioice & M	ge from agon asumer ity, r IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Networking in APQ8009, APQ8017, APQ8013, APQ8017, APQ8013, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9607, MDM9605, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150   CVE ID: CVE-2019-2297	Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	CID
Out-of-bounds Read  Out-of				APQ8 APQ8 IPQ40 MDM' MDM' MSM8 QCA6 QCA9 QCS40 SDA8 SDM8 SM81	017, APC 064, APC 019, IPQS 9206, MI 9650, MI 9650, MI 379, QCI 05, QCS6 45, SDM 145, SDX	Q8053, Q8096A Q8096A B064, IP DM9207 DM9640 SM8905 QCA617 QCA937 N7605, S05, SDA 636, SDA 20, SDX2	U, Q8074, 'C, ), , 74A, 7, .660, M660, 24,				
When it receives malformed   XID message. in Snapdragon   Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8937, MSM8939, MSM8940, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,											
- II-I I I-X X-4 X-4 X-5 X-6 X-7 X-9 Y-11 X-9		21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Weara APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8 MSM8	out side it receive lessage. Snapdra dragon Indragon Indr	its bour res malfo in Snapo agon Cor onsume dustria oT, Snap ragon V ragon APQ800 Q8053, APQ809 DM9605 DM9625 DM9625 DM9625 MB9676, MSM891 SM8940, SM8976, MSM89 2150, Q0	ndary ormed dragon npute, r IOT, l IOT, dragon oice &  9,  8,  6,  7,  17,  28,  17,  298,  CS605,	w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	•	
(CVSS)	_	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	dragon_H 1130, SXI <b>D : CVE-</b>	630, SD 660, SD 845, SD 5, SDX55 150, SM High_Me R2130 <b>2019-2</b>	M632, M670, M850, , 8150, d_2016				
N/A	21-11-2019	7.2	copy to the Paramare from Environment of Snapor Sna	e invoking from fd of a secure be neters be om non soment. Snapdradragon Colragon Indragon Williagon Williagon, MS 3905, MS 3905, MS 3905, MS 3905, MS 3905, MS 3906, SDA 600, SDA 6	or local bouffer, eing pope secure in Snape gon Coronnectivonsume adustria lobile, oice & More and a APQ80 (28053, Q8096A) (28096A) (28096	ouffer oulated dragon inpute, vity, r IOT, l	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-9 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	l	Description	on & CVE	ID	Pat	ch	NCIIP	CID
			, SXR1	50, lragon_F l 130, SX <b>D : CVE-</b>	R2130					
Use After Free	21-11-2019	7.2	cleand missing for a fapplic Comp Consu Indus Mobil Infras Netwo QCS40 SDM6 SDX55 SM81	fter free up routing points failed station. in ute, Snap trial IOT e, Snap detructure orking ir 04, QCS6, SM615, SM615, SM615, SXR1	ne due to er saniti ort of a to Snapdr pdragon C, Snapdo Ragon W e and on MDM9 605, SDA 1710, SD 1710, SX	zation rusted ragon ragon vired 205, .845, M845, 150, CR2130	https:/w.qualm.com pany/jct- securite lletins ber-20 bulleti	ty/bu /octo	O-QUA-9 031219	
mdm9206_fir	mware									
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi- result in Sna Snapo Snapo Snapo Mobil Music Weara APQ8 APQ8 MDM' MDM' MDM' MDM'	e process t messag tion is no ing into pdragon C dragon I dragon I dragon I e, Snapdr e, Snapdr ables in A 017, APC 096AU, A 9150, MI 9635M, I 9635M, I 9635M, I	ge, Valid ot met an infin Auto, ompute, onsume off, Snap Aragon Vagon APQ800 Q8053, APQ809 DM9607 DM9607 DM9607	exit ite loop  r IOT, l IOT, dragon oice &  9,  8, 5, 7, 5, 40,	https:/ w.qual m.com pany/j ct- securir lletins ber-20 bulleti	ty/bu /octo	O-QUA- MDM9- 031219	/461
			MDM9650, MDM9655,  2-3 3-4 4-5 5-6				1			

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	3905, MS 3909W, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDM 530, SDM 545, SDM 55, SM615 50, SM82 dragon_H	MSM891, M8937, M8953, M8996, Sobar, S605, Q1632, SD632, SD605, SD605, SD605, SM7250, S	AU, M215, A845, M450, M636, M710, X20,				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race of lack of will be modified stater bound Auto, Electric Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MSM8 MSM8 MSM8 MSM8 QCN7	condition of resource concurfied in the ment leaded access in Snapdra dragon Indragon Indrago	n due to ce lock we rently e memo dis to out in Snape gon Coronsume dustria pragon Vagon APQ800 Q8053, APQ809 QM9207 QM9640 GM8905 MSM8936 Cobar, G405, Q0	the which  py t of dragon issumer ity, r IOT, dragon oice &  9,  8, 7C, 0, , 89, AU,	https:/ w.qual m.com pany/ct- securit lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- MDM9- 031219	/462
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
				SDM6 SDM7 SDX2 SM81	129, SDM 532, SDM 710, SDM 4, SM61 50 ( <b>D : CVE</b> -	1636, SD 1845, SD 50, SM7	M660, X20, 150,				
Use After Free	21-	-11-2019	2.1	daem static freed in Sna Snape Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SM61 SM82	fter free ton shute object in from a rapdragon of dragon	down dunstance in Auto, compute connectificonsume ragon APQ800 Q8053, APQ809 GM8905 GM	e to getting places  , vity, er IOT, l IOT, dragon oice &  9,  8,  6,  77,  W,  CS605, M450, M710, 24, 8150,	https:/w.qualm.com pany/ct- securilletins ber-20 bulleti	ty/bu /octo	0-QUA- MDM9- 031219	/463
Improper Validation of Array Index	21-	-11-2019	4.6	occur to im	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon https:/  m.qual m.com			lcom l/com	O-QUA- MDM9- 031219	/464	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Electr Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM' MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDX2	Snapdra conics Co dragon In dragon W dragon W dragon W 009, APO 053, APO 098, MD 9207C, M 9640, MS 3905, MS 3905, MS 3909W, N 3996AU, 605, SDM 605, SDM 0	onnectivonsume ndustria Iobile, Ioice & Novearable Q8017, Q8096A M9206, MDM9650 MSM891, MSM891, MSM8931, MSM8931, MSM8931, MSM8931,	ity, er IOT, l IOT,  Music, es in  U,  17, 17, 18, 198, 180, 186, 186, 186,	ct- securii lletins ber-20 bulleti	octo 19-		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer wlan rates elementhan rates Snapo APQ8 APQ8 MDM MDM MSM8 QCA6	r overflomodule is or extendent length max rate dragon Caragon Caragon Indragon Waragon Warago	w can of supponded rate has great lenguato, ompute onsume	ccur in rted es ater gth in rty, r IOT, I IOT, Music in 06,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	/465
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130		
			CVE ID : CVE-2019-10566		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MDM9- 031219/466
			CVE ID : CVE-2019-2266		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MDM9- 031219/467
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MSM8 QCA6 QCA9 SDA6 SDM6	9207C, M 9650, M 8998, QC 574AU, 379, QC 60, SDM 660, SDM 845, SDX <b>D : CVE</b> -	SM8996 CA6174 <i>F</i> QCA937 S405, QO 630, SD I670, SD 20, SM6	AU, A, 7, CS605, M636, M710, 150				
Out-of- bounds Read	21-11-2019	10	while session messar un-in Snapo Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	r over reparsing on manages if no tended with the design of the design o	downlingement etwork stalues in auto, compute consume ndustria oT, Snaphragon Vagon APQ800 DM9605 DM9605 DM9605 DM9605 DM9655 SM8909 MSM8937 SM8940 BMSM8937 SM8940 BMSM8937 SM8940 BMSM8937 SM8940 BMSM893 SM8940 BMSM893 SM8940 BMSM893 SM8940 BMSM893 SM8937 SM8940 BMSM893 SM8940 BMSM893 SM8940 BMSM893 SM893 SM8940 BMSM893 SM893 SM8940 BMSM893 SM8940 BMSM893 SM8940 BMSM893 SM893	nk OTA sends  , er IOT, el IOT, odragon oice & 09, 40, 5, 40, 5, 40, 6, 6, 40, 6, 6, 40, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	https://w.qualm.com/pany/jct-securitelletins/ber-20/bulletins/	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/468
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			SM61 SM82 Snapo , SXR2	0, SDX24 50, SM7 50, dragon_H 1130, SX <b>D : CVE-</b>	150, SM Iigh_Me R2130	8150, d_2016				
Improper Authenticati on	21-11-2019	10	Lack of allow NAS in result bypas Snapo Snapo Snapo Snapo Mobil Music Wear, APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integrals MODER nessages into autorises of NAS dragon Adragon Coloragon In dragon I	ity check M to accombined to chentical in uto, ompute, onsume industrial oT, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9625 MDM9655 SM8909, MSM891 SM8937, SM8940, SM8976, MSM891 SM891 SM89	ept any can tion for IOT, dragon to	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	/469
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			^	lragon_F l 130, SX	0 –	d_2016				
			CVE I	D : CVE-	2019-2	289				
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electric Snape Sn	r overfloor process and NAN space. in Snapdra conics Coloragon In dragon In dragon Vertructure orking in 19, IPQ 19, I	ing non- I message Snapdra agon Cor connective consume ndustria Mobile, Voice & M Vired e and n APQ80 Q8053, Q8096A 8064, IP DM9640 SM8905 QCA617 QCA937 N7605, 605, SDA 636, SDA	ge from agon asumer ity, r IOT, l IOT	https:/ w.qual m.com pany/j ct- securing lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil	P modul out side it receiv lessage. Snapdra dragon C dragon Id dragon Id e, Snapdra	eits bour ves malfo in Snapo agon Cor consume ndustria oT, Snap Iragon V	ndary ormed dragon npute, r IOT, l IOT, dragon	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/471
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Weara APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	ables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 3905, MS 3905, MS 3905, MS 3996AU, 45, SC818 45, SC818 45, SDM 45, SDM 45, SDM 710, SDM 710, SDM 710, SDM	APQ800 Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 SM8909, MSM8916, SM8976, MSM89 2150, Q0 80X, SDA 429, SDI 1630, SD 1660, SD 1660, SD 1845, SD 150, SM High_Me R2130	9, 8, 6, 7, 40, 6, 7, 98, CS605, A660, M439, M632, M670, M850, , 8150, d_2016			T.C.III	
N/A	21-11-2019	7.2	copy for the the Param are from	e invokin from fd o secure l neters be om non s onment. Snapdra dragon C dragon C dragon V dragon V structure orking ir	or local buffer, eing popsecure in Snapelogon Corsonsumendustria Mobile, Voice & Movined e and	ouffer oulated dragon npute, vity, r IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
mdm9607_fir	mware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MDM9- 031219/473

3-4

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	3905, MS 3909W, I 3920, MS 3940, MS 3976, MS 3998, Nio 2150, QC 30X, SDM 229, SDM 30, SDM 345, SDM 345, SDM 35, SM61! 50, SM8 Iragon_H	MSM8937, SM8937, SM8996, cobar, S605, Q A660, SD I632, SD I632, SD I670, SD I850, SM7 250, High_Me	M215, A845, M450, M636, M710, X20,				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race of lack of will be modified stater bound Auto, Electron Snape Mobil Music Wears APQ8 APQ8 MDM MDM MDM MSM8 MSM8 MSM8 QCN7	D: CVE- condition f resour e concur fied in the ment lead d access Snapdra conics Co dragon I	n due to ce lock we rently de memo ds to out in Snape agon Cor onsume ndustria oT, Snape lragon V ragon APQ809 DM9207 DM9640 SM8905 MSM893 cobar, S405, Q0	the which py t of dragon ity, or IOT, dragon oice & 9, 8, 7C, 9, 89, AU, CS605,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	/474
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
				SDM6 SDM7 SDX2 SM81	129, SDM 532, SDM 710, SDM 4, SM61 50	1636, SD 1845, SD 50, SM7	M660, X20, 150,				
Use After Free	21-	-11-2019	2.1	Use a daem static freed in Snape Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM8 SM61 SM82	fter free and shute a object in from a reapdragon of dragon of dra	issue in down dunstance in Auto, Compute Connections and Consume Industria oT, Snap Iragon Vagon APQ800 Q8053, APQ809 GM8905 GM8905 GM8905 GM8939, GM8939, GM8953, GM8	Xtra e to getting places  vity, r IOT, l IOT, dragon oice &  9,  8,  7,  W,  AU, CS605, M450, M710, 24, 8150,	https://w.qualm.com/pany/jct-securitelletins/ber-20	ty/bu /octo	O-QUA- MDM9- 031219	/475
Improper Validation of Array Index	21-	-11-2019	4.6	occur to im	of-bound in came proper v index in	era drive ralidatio	r due n of	https://w.qual m.com pany/	lcom l/com	O-QUA- MDM9- 031219	/476
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			Electr Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM' MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDX2	Snapdra conics Co dragon Indragon Wilragon Wilragon Wilragon Wilragon Wilragon Wilragon Wilragon Wilragon Wilragon, MS 1905, MS 1905, MS 1905, MS 1906, SDM 1906, SD	onnectivonsume onsume onsume onsume onsume onsume on ons	ity, er IOT, l IOT,  Music, es in  U,  17, 17, 18, 198, 100450, 10660,	ct- securii lletins ber-20 bulleti	octo )19-		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer wlan rates elementhan rates Snapo APQ8 APQ8 MDM MDM MSM8 QCA6	r overflomodule in or extendent length has rate dragon Adragon Conics Co	w can or of supported the supp	ccur in rted es ater gth in rty, r IOT, I IOT, Music in 06,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	/477
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130		
			CVE ID : CVE-2019-10566		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MDM9- 031219/478
			CVE ID : CVE-2019-2266		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MDM9- 031219/479
CV Scoring Scal (CVSS)	e 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MSM8 QCA6 QCA9 SDA6 SDM6	9207C, M 9650, M 8998, QC 574AU, 379, QC 60, SDM 660, SDM 845, SDX <b>D : CVE</b> -	SM8996 CA6174 <i>F</i> QCA937 S405, QO 630, SD 1670, SD 20, SM6	AU, 7, CS605, M636, M710, 150				
Out-of- bounds Read	21-11-2019	10	while session messar un-in Snapo Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	r over reparsing on manages if no tended with the design of the design o	downlingement etwork stalues in auto, compute consume ndustria oT, Snaphragon Vagon APQ800 DM9605 DM9605 DM9605 DM9655 SM8909 MSM8937 SM8940 BMSM8937 SM8940 BMSM8937 SM8940 BMSM8937 SM8940 BMSM8937 SM8940 BMSM8937 SM8940 BMSM893 SM8937 SM8940 BMSM893 SM8937 SM8940 BMSM893 SM8940 SM8937 SM8940 SM8937 SM8940 SM8937 SM8937 SM8940 SM	nk OTA sends  r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, 40, 6, M439, M632, M670,	https://w.qualm.com/pany/jct-securitelletins/ber-20/bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/480
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness F	Publish Date	cvss		Description	on & CVE	Pat	ch	NCIIP	CID	
			SM61 SM82 Snapo	0, SDX24 50, SM7 50, lragon_H 130, SX	150, SM ligh_Me	8150,				
			CVE I	D : CVE-	2019-2	271				
Improper Authenticati on 2	1-11-2019	10	allow NAS result bypas Snapo Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integrals MODE of integrals MODE of integrals and services of NAS dragon of the control of th	M to accis which of thentical suto, compute on sume houstrian of the consume of the consumer of the consum	ept any can cion rion, I IOT, dragon oice & 9, 40, 7, 7, 186600, 186600, 186600, 186600, 186600, 186600, 186600, 186600, 186600, 186600, 186600, 186600, 186600, 186600, 186600, 186600, 1866000, 186600, 186600, 1866000, 1866000, 1866000, 1866000, 18660000, 1866000, 1866000, 1866000, 1866000, 1866000, 1866000, 1866000	https:/w.qualm.company/jct-securitelletins/ber-20bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219,	/481
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			^	lragon_F L130, SX	<b>U</b> –	d_2016				
			CVE I	D : CVE-	2019-2	289				
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electric Snapo Snapo Snapo Snapo Infras Network APQ8 APQ8 IPQ40 MDM MDM MDM MSM8 QCA6 QCA9 QCS40 SDA8 SDM8 SM81	r overfloor process and NAN space. in Snapdra conics Coloragon In dragon In dragon Vertructure orking in 19, IPQ 19, I	ing non- imessage Snapdra igon Cor onnective onsume industria Mobile, Vired e and APQ80 Q8053, Q8096A B064, IP DM9640 SM8905 QCA617 QCA937 N7605, 505, SDA 636, SDI 20, SDX	ge from agon asumer ity, r IOT, l IOT	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/482
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil	P modul out side it receiv lessage. Snapdra dragon I dragon I dragon I e, Snapd	its bour res malfo in Snapo agon Cor onsume ndustria oT, Snap Iragon V	ndary ormed dragon npute, r IOT, l IOT, dragon	https://w.qualm.com/pany/jct-securingletins/ber-20	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/483
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Weara APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	ables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 3905, MS 3905, MS 3905, MS 3939, MS 3953, MS 3	APQ800 Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 SM8909, MSM8916, SM8976, MSM89 2150, Q0 80X, SDA 429, SDI 1630, SD 1660, SD 1660, SD 1845, SD 150, SM High_Me R2130	9, 8, 6, 7, 40, 6, 7, 98, CS605, A660, M439, M632, M670, M850, , 8150, d_2016			T.C.III	
N/A	21-11-2019	7.2	copy for the the Param are from	e invoking from fd of secure landers be om non somment. Snapdra dragon Calragon Calragon Calragon Waragon Wara	or local buffer, eing popsecure in Snapelogon Corsonsumendustria Mobile, Voice & Movined e and	ouffer oulated dragon npute, vity, r IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
mdm9650_fir	mware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MDM9- 031219/485

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	3905, MS 3909W, I 3920, MS 3940, MS 3976, MS 3998, Nio 2150, QC 30X, SDM 229, SDM 30, SDM 345, SDM 345, SDM 345, SM	MSM8937, SM8937, SM8953, SM8996, cobar, S605, Q A660, SD I632, SD I632, SD I670, SD I850, SM7 250, High_Me	M215, A845, M450, M636, M710, X20,				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race of lack of will be modified stater bound Auto, Electron Snape Mobil Music Wears APQ8 APQ8 MDM MDM MDM MSM8 MSM8 MSM8 QCN7	D: CVE- condition f resour e concur fied in the ment lead d access Snapdra conics Co dragon I	n due to ce lock werently le memods to our in Snape on Coronsume of Consume o	the which py t of dragon ity, or IOT, dragon oice & 9, 8, 7C, 9, AU, CS605,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	O-QUA- MDM9- 031219	/486
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
				SDM6 SDM7 SDX2 SM81	129, SDM 532, SDM 710, SDM 4, SM61 50 <b>D : CVE</b> -	1636, SD 1845, SD 50, SM7	M660, X20, 150,				
Use After Free	21-	-11-2019	2.1	Use a daem static freed in Snape Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM8 SM61 SM82	fter free on shute object in from a rapdragon of dragon	issue in down dunstance in Auto, Compute Connections and Consume Industria oT, Snap Iragon Vagon APQ800 Q8053, APQ809 GM8905 GM8905 GM8905 GM8939, GM8939, GM8953, GM8	Xtra e to getting places  vity, er IOT, l IOT, dragon oice &  9,  8,  7,  W,  AU, CS605, M450, M710, 24, 8150,	https:/w.qualm.com/pany/ct-securilletinsber-20	ty/bu /octo	0-QUA- MDM9- 031219	/487
Improper Validation of Array Index	21-	-11-2019	4.6	occur to im	of-bound in came proper v index in	era drive ralidatio	r due n of	https:/ w.qual m.com pany/	lcom l/com	O-QUA- MDM9- 031219	/488
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			Electr Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM' MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDX2	Snapdra Snapdra Tonics Co dragon C dragon M dragon W 009, APO 053, APO 098, MD 9207C, M 9640, MI 3905, MS 3905, MS 3905, MS 3905, MS 3905, MS 3905, MS 3905, MS 3905, MS 300, SDM 0 D: CVE-	onnectivonsume on sume	ity, er IOT, el IOT,  Music, es in  U,  07, 17, 17, 18, 198, 0M450, 0M660,	ct- securii lletins ber-20 bulleti	octo )19-		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer wlan rates elementhan rates Snapo APQ8 APQ8 MDM MDM MSM8 QCA6	r overflomodule in or extendent length has rate dragon Chagon Chagon Indragon Words (17, APC) (174A, QC) (174A, QC) (177, QC) (177, QC) (177, QC)	w can of supponded rate has great lenguato, ompute onsume	ccur in rted es ater gth in rity, er IOT, al IOT, Music in 06,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	O-QUA- MDM9- 031219	/489
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			SDA8 SDM8	605, QC: 45, SDM 45, SDX 50, SM8	670, SD 20, SM6	M710, 150,				
			CVE I	D : CVE-	2019-1	0566				
Out-of- bounds Read	21-11-2019	7.5	P2P a handl mana Snapo Snapo Snapo Snapo APQ8 APQ8 MDM MSM8 QCA6 QCA9 SDA6 SDM6	ole OOB ction fra ing WLA gement : dragon A dragon C dragon I dragon M dragon W 009, AP 009, AP 0098, MD 09207C, M 9650, M: 379, QC 60, SDM 60, SDM	imes whan Inframe in Luto, Consume Industria Mobile, Wice & M Q8017, Q8096A MM9206, MDM960 SM8996 CA6174A QCA937 S405, QC	ile  r ity, r IOT, l IOT, Music in  U, A, 7, CS605, M636, M710,	https:/ w.qual m.com pany/ ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	
			CVE I	D : CVE-	2019-2	268				
Out-of- bounds Read	21-11-2019	10	while session messa un-int Snapo Snapo Snapo Snapo Snapo Mobil	r over reparsing manages if ne tended valued of the decident o	downlingement of the setwork so walues in the setwork so walues in the setwork so wall and the setwork	ortA eends r IOT, l IOT, dragon	https://w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	ables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MS 3905, MS 3905, MS 39953, MS 3953, MS	APQ800 Q8053, APQ809 DM9607 DM9605 DM9655 MB909, MSM8916, MSM8937, GM8940, GM8976, MSM8940, GM8976, MSM89 EM8976, MSM8910, GM8976, G	9, 8, 5, 40, 5, 40, 6, 7, 68, 6805, 6860, 6832, 6832, 6850, 6850, 68150, 68150, 68150,				
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	dragon_F 1130, SX	DM9607 DM9625 MDM9655 MB909, MSM8916 SM8940, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDA 429, SDA 1660, SD 1845, SD 150, SM High_Me R2130	7, 40, 5, 40, 5, 17, 98, CS605, A660, M439, M670, M670, M850, 5,				
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electr Snapo Snapo Snapo Infras Network APQ8 APQ8 IPQ40 MDM	Buffer overflow can occur while processing non- standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,		https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/493	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID: CVE-2019-2297							
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8 MSM8	P modulout side it receives sage. Snapdradragon Idragon Idragon, MI 19635M, MI 196	its bour yes malfo in Snapo agon Cor onsume ndustria oT, Snapo lragon V ragon APQ809 DM9607 DM9607 DM9625 MDM9655 SM8909, MSM891 SM8937, SM8940, MSM89	ndary ormed dragon npute, r IOT, l IOT, dragon oice &  9,  8,  7,  40,  7,	https:/ w.qual m.com pany/ct- securit lletins ber-20 bulleti	ty/bu /octo	O-QUA- MDM9- 031219,	/494
			SDA8 SDM4 SDM6 SDM7 SDX2	.5, SC818 45, SDM .50, SDM .36, SDM 10, SDM 0, SDX24 50, SM7	429, SD1 1630, SD 1660, SD 1845, SD 1, SDX55	M439, M632, M670, M850,				
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
Weakness	Publish Date	CVSS	SM82 Snapo , SXR2 CVE I  While copy to the Param are fr envire Auto, Snapo Snapo Snapo Snapo Snapo Snapo	50, dragon_H 1130, SX D: CVE- invoking from fd of secure le neters be om non: Snapdra dragon Collagon Collagon M dragon W dragon W	Aligh_Med R2130 2019-2 g the AF or local bouffer, eing pop secure in Snapo gon Cor onnectivonsume ndustria lobile, foice & M	d_2016  303 PI to ouffer oulated dragon inpute, vity, r IOT, I IOT,	Pat	ch	NCIIP	CID
N/A	21-11-2019	7.2	Infras Netwo APQ8 APQ8 APQ8 MDM MSM8 MSM8 MSM8 MSM8 QCS4 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6	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, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130				//ww lcom l/com produ ty/bu /octo 019- n	O-QUA- MDM9- 031219	/495
mdm9655_fir	mware									
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9635M, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MDM9- 031219/496
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in	https://ww w.qualcom m.com/com pany/produ ct-	O-QUA- MDM9- 031219/497
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
WEARITESS	T UDIISII Date	CV33	Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musio Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	dragon Adragon Colragon Colragon Indicated Ind	auto, ompute, onsume dustria oT, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9605 SM8909, MSM891 SM8937, SM8940, SM8976, MSM8976, MSM89 2150, Q0 30X, SDA 429, SDI 660, SD	r IOT, l IOT, dragon oice & 9, 8, 40, 5, 40, 5, 40, 5, 40, 6, M632, M632, M670, M850, , 8150,	securit lletins, ber-20 bulleti	ty/bu /octo 19-	NGIII	
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,			https://w.qualm.com pany/jct- securit lletins/ber-20	com /com produ ty/bu /octo	O-QUA- MDM9- 031219		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Snapo Snapo Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	dragon Indragon Indragon Idragon Idrag	ndustria oT, Snap ragon V ragon APQ800 Q8053, APQ809 DM9605 DM9655 MDM965 DM9655 MSM8916, MSM8916, MSM8976, MSM	l IOT, dragon foice & 9, 8, 5, 40, 5, 40, 6, 4660, M439, M632, M670, M850, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	bulleti			
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,				https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303		
msm8996au_	firmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/500

CV Scoring Scale

6-7

7-8

8-9

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130							
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modified stater bound Auto, Electron Snape Mobil Music Wears APQ8 APQ8 MDM	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640,			https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	/501
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID: CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/502

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM896AU, MSM898, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/503
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/504

3-4

4-5

6-7

5-6

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID: CVE-2019-10535		
Out-of- bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/505
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/506
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish D	ate	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
				MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	9650, M. 8996AU, 174A, Q. 377, QC. 605, QC. 45, SDM 845, SDX 50, SM8	Nicobar CA6574 A9379, S405, Q0 670, SDI 20, SM6 250, SXI	CS605, M710, 150, R2130				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-20	019	7.2	from source that to potent buffer Snape Sn	tmap file any un-a te, there he bitma atially ca r overflo dragon C dragon C dragon C dragon I dragon I dragon I dragon I dragon V 5016, AP 5098, MD 6098, MD 645, SDM 645, SDM 650, SDM 650, SM7 650, SM7	is a possing can use stack w. in auto, compute connective consumendustria Mobile, Mos	cated sibility k  k  vity, er ity, l IOT, l	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/507
Out-of- bounds Read	21-11-20	019	7.5	P2P a handl mana	ble OOB ction fra ling WLA gement dragon A	imes wh AN frame in	ile	https://w.qual m.com pany/j	com /com	O-QUA- MSM8- 031219	/508
CV Scoring Scal (CVSS)	e <b>0-1</b>		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			Electr Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 SDA6 SDM6	dragon Conics Co	onnectivonsume ndustria lobile, loice & M Q8017, Q8096A M9206, MDM960 SM8996 A6174A QCA937 S405, QO	ity, or IOT, l IOT, fusic in U, O7, AU, A, 7, CS605, M636, M710,	securit lletins ber-20 bulleti	octo )19-		
			CVE I	D : CVE-	2019-2	268				
Out-of- bounds Read	21-11-2019	10	while session messar un-information of the session messar un-information of the session of the s	r over reparsing manages if netended valuagen Caragon Caragon Internation Inte	downlingement of tworks alues in uto, ompute onsume ndustria oT, Snap ragon Vagon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9655 MB9695 MSM891	nk OTA sends  r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5,	https:/ w.qual m.com pany/j ct- securing lletins ber-20 bulleti	ty/bu /octo	0-QUA- MSM8- 031219	/509
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX20 SM61 SM82 Snapo	3939, MS 3953, MS 3996AU, ar, QCM 5, SC818 45, SDM 50, SDM 10, SDM 50, SM7 50, SM7 50, lragon_H	SM8976, MSM89 2150, Q0 30X, SDA 429, SDI 630, SD 660, SD 845, SD 7, SDX55 150, SMS	98, CS605, A660, M439, M632, M670, M850, ,				
Improper Authenticati on	21-11-2019	10	Lack of allow. NAS in result bypas Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integris MODEN nessages into aut s of NAS dragon A dragon C dragon I dra	ity check M to accombined to chentical in uto, ompute, onsume adustria oT, Snap ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MDM9625 MDM9625 MDM9625 MB909, MSM8916, SM8940, SM8940,	ept any can tion  r IOT, l IOT, dragon oice &  9,  8,  7,  40,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/510
CV Scoring Scale			IAIOIAI	JJJUHU,	MOMENT	70,				

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			QM21 SDA8- SDM6 SDM7 SDX2- SM61 SM82 Snapo	ar, QCM 5, SC818 45, SDM 50, SDM 710, SDM 710, SDX24 50, SM7 50, 1ragon_H 1130, SX D: CVE-	80X, SDA 429, SDI 630, SD 6660, SD 845, SD 150, SM High_Me R2130	A660, M439, M632, M670, M850, 8150,				
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electric Snape Sn	r overflooprocess, and NAN space, in Snapdra conics College of the space of the spa	ing non- messag Snapdra gon Cor onsume ndustria Mobile, foice & M Vired and APQ80 Q8053, Q8096A B064, IP DM9640 SM8905 QCA617 QCA617 QCA937 N7605, S05, SDA 636, SDI 20, SDX	ge from agon isumer ity, or IOT, IOT, Iusic, Q8074, 7C, 9, 74A, 7, 4660, M660, 24,	https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	com l/com produ ty/bu /octo	0-QUA- MSM8- 031219	/511
Out-of-	21-11-2019	7.5	SNDC	P modul	e may a	ccess	https:/	//ww	O-QUA-	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	n & CVE	ID	Pat	ch	NCIIP	CID
bounds Read			array	out side	its bour	ndary	w.qual	com	MSM8-	
			when	it receiv	es malfo	ormed	m.com	/com	031219	/512
			XID m	iessage. i	in Snapo	dragon	pany/	produ		
				Snapdra	•	•	ct-			
			•	lragon C			securi			
			•	lragon Ir			lletins			
			•	lragon Io	•	•	ber-20			
				e, Snapd	_	oice &	bulleti	n		
				, Snapdr	•					
				ables in A	•	9,				
				017, AP(	•	_				
			_	096AU, A	-					
				9150, MI		•				
				9206, MI		•				
				9615, MI		•				
				9635M, I		•				
				9650, MI						
				3905, MS						
				3909W, I		•				
				3920, MS	-					
				3939, MS 3953, MS	•					
				3933, M3 3996AU,	-					
				ar, QCM		•				
				.5, SC818						
			_	45, SDM						
				50, SDM	•	•				
				36, SDM		•				
				10, SDM	•	•				
				0, SDX24	•	•				
				50, SM7						
			SM82		100,011	0 2 0 0,				
				lragon_F	ligh Me	d 2016				
			_	130, SX	_	_				
			-	D : CVE-		303				
			While	invokin	g the AF	PI to	https:/	//ww		
				from fd c	_		w.qual		0.0114	
NI / A	21 11 2010	7.2		secure l		-	m.com		O-QUA- MSM8-	
N/A	21-11-2019	7.2		neters be	•	ulated	pany/			/510
				om non s	• • •		ct-	-	031219	7515
				onment.		dragon	securi	ty/bu		
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	<u> </u>		_ 3	202	. 3		_	, 0		J 10

Weakness	Publish Date	CVSS	ı	Descriptio	on & CVE	ID	Pat	ch	NCIII	PC ID
			Snapo Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 APQ8 APQ8 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDA66 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SNapo SDM8 SDM8 SDM8 SDM8 SDM8 SDM8 SDM8 SDM8	Snapdra Snapdra Iragon C Iragon II Iragon W Iragon M Irag	onnective on sume and ustrial flobile, foice & Movined and and and APQ80 (28053, 28096A) (28096A) (280	vity, r IOT, l IOT, lusic,  09, U, 5, 0, 429, M630, M660, M845, 7150, d_2016	lletins, ber-20 bulleti	19-		
Out-of- bounds Read	21-11-2019	2.1	Trusta memo result Snapo Snapo Snapo Snapo Snapo Snapo Snapo	ecure Kozone to Cory read into DO Iragon Colragon Iragon Worgon Worden	do an ar' which w S in uto, onnectiv onsume ndustria Jobile, Joice & M	bitrary vill vity, r IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318		
mdm9615_fir	mware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MDM9- 031219/515

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDM8 SDX5 SM81 Snapo	30, SDM 660, SDM 845, SDM 5, SM61! 50, SM8 dragon_F 1130, SX <b>D : CVE</b> -	1670, SD 1850, SD 50, SM7 250, High_Me R2130	M710, X20, 150, d_2016				
Out-of- bounds Read	21-11-2019	10	while session messarun-in Snapo Snapo Snapo Snapo Mobil Music Wear, APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	r over reparsing on manages if no tended with the design of the design o	downlingement of tworks aralues in auto, compute consume adustria of the consume aragon of the consumer are consum	nk OTA ends  r IOT, I IOT, dragon foice &  9,  8,  6,  7,  40,  6,  40,  6,  40,  6,  M439,  M632,  M670,  M850,	https:/w.qualm.com pany/jct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/516
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

SM6150, SM7150, SM8150, SM8250, Snapdragon, High, Med_2016	Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Iot, Snapdragon Wearables in APQ8009, APQ8017, APQ8098, MDM9150, MDM9205, MDM9205, MDM9205, MDM9615, MDM9625, MDM9615, MDM9625, MDM9650, MDM965				SM82 Snapo	50, lragon_F	ligh_Me	·				
Allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Ioft, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8017, APQ8053, APQ8017, APQ8096, MDM9206, MDM9206, MDM9206, MDM9206, MDM9206, MDM9615, MDM9625, MDM9635M, MDM9625, MDM9635M, MDM9655, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8996, MSM8917, MSM8920, MSM8937, MSM8933, MSM8940, MSM8937, MSM8933, MSM8940, MSM8933, MSM8940, MSM8933, MSM8940, MSM8933, MSM8940, MSM8996, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM620, SDM630, SDM632, SDM636, SDM660, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM630, SDM632, SDM636, SDM660, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016				CVE I	D : CVE-	2019-2	271				
1 1-1 1-1 1-3 1 3-4 1 4-5 1 5-6 1 6-7 1 7-8 1 8-9 1 9-111	Authenticati	21-11-2019	10	allow NAS r result bypas Snapo Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	s MODEl nessages into autis of NAS dragon Adragon Idragon Idra	M to accomb to accomb the microstrial of the micros	ept any can tion  r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 6, 47, 4660, 4439, 4660, 4660, 4660, 4660, 4650,	w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	MDM9-	/517
	CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Out-of-bounds Read  Name Map Out-of-bounds Read  Name Map Out-of-bounds Read  Out-of-bounds Read  Name Map Out-of-bounds Read  Name Map Out-of-bounds Read  Out-of-bounds Read  Name Map Out-of-bounds Read  Name Map Out-of-bounds Read  Name Map Out-of-bounds Read  Name Map Out-of-bounds Read  Out-of-bounds Read  Name Map Out-of-bou
SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9650, MDM9650, MDM9650, MSM8909, MSM8909, MSM8917, MSM8905, MSM8909, MSM8917, MSM8908, MSM8917, MSM8939, MSM8940, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM896AU, MSM896AU, MSM898, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM630
array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9206, MDM9615, MDM9205, MDM9206, MDM9655, MDM9615, MDM9625, MDM9615, MDM9655, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8939, MSM8940, MSM8939, MSM8940, MSM8939, MSM8940, MSM8939, MSM8940, MSM8953, MSM8976, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA660, SDA660, SDA660, SDA660, SDA660, SDA660, SDA660, SDM670, SDM710, SDM845, SDM8250, SDX20, SDX24, SDX24, SDX55, SM6150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130
mdm9625_firmware

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condiresult in Snape Snape Snape Snape Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	e process t messag tion is n ing into apdragon of dragon of dragon Id dragon Id dragon Id e, Snapdra ables in 017, APO 096AU, 19 150, M 9635M, 19 9635M, 19	ge, Valid ot met an infin n Auto, compute consume ndustria oT, Snap lragon V ragon APQ809 DM9607 DM9607 DM9655 MDM9655 SM8909, MSM8937, SM8953, SM8953	exit ite loop , er IOT, el IOT, el IOT, edragon oice &  9,  8, 5, 7, 5, 40, 5, 17, AU, M215, M450, M636, M710, X20, 150, d_2016	https:/w.qualm.company/jct-securitelletins/ber-20/bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	/519
Out-of- bounds Read	21-11-2019	10	while sessio messa	r over re parsing on manag ages if ne tended v	downlii gement etwork s	nk OTA sends	https:/ w.qual m.com pany/j	com /com	0-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musio Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	dragon Adragon Colragon Indicated Inagon Indicated Inagon Indicated Inagon Indicated Inagon I	auto, ompute, onsume dustria oT, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9605 SM8909, MSM891 SM8937, SM8940, SM8976, MSM8976, MSM89 2150, Q0 30X, SDA 429, SDI 660, SD	r IOT, l IOT, dragon oice & 9, 8, 40, 5, 40, 5, 40, 6, M439, M632, M670, M850, , 8150,	securit lletins, ber-20 bulleti	ty/bu /octo 19-		
Improper Authenticati on	21-11-2019	10	allow NAS result bypas Snapo Snapo	of integra s MODEI nessages into aut ss of NAS dragon A dragon C	M to accombined to the second of the second	ept any can tion	https://w.qualm.com pany/jct- securit lletins/ ber-20	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDA84 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	lragon_H 130, SX <b>D : CVE-</b>	oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9607 DM9625 MDM9655 SM8909, MSM891 SM8937, SM8940, SM8976, MSM89 2150, Qu 80X, SDA 429, SDI 1660, SD 1660, SD 1660, SD 1660, SD 1650, SM	dragon foice & 9, 8, 5, 7, 6, 40, 6, 7, 40, 6, 4660, 439, 4670, 4670, 4670, 4670, 6150, 61	bulleti	n		
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil	P modul out side it receiv essage. Snapdra Iragon I Iragon I e, Snapd , Snapdr	its bour res malfo in Snapo agon Cor onsume ndustria oT, Snap Iragon V	ndary ormed dragon npute, r IOT, l IOT, dragon	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/522
			Weara	ables in A	APQ800	9,				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303		
mdm9205_fir	mware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, 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/october-2019-bulletin	O-QUA- MDM9- 031219/523

3-4

2-3

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM898, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2335							
Use After Free	21-11-2019	4.9	listen memo use af Snapo	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID: CVE-2019-2336			https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	/524
Improper	21-11-2019	7.2	Out o	f bound a	access d	ue to	https:/	//ww	O-QUA-	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Restriction of Operations within the Bounds of a Memory Buffer			array image Snape	f check of size white elf segn Adragon Chagon Chagon Indragon Indragon Working in 104, QCS 6, SDX 130, SXR	le readinents. in uto, ompute onnectionsume dustrial MDM9 and 1710, SDA 1710, SDA 150, SM	ng the vity, r IOT, l IOT, 205, 845, M845,	w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	/com produ ty/bu /octo 119-	MDM9- 031219,	/525
			CVE I	D : CVE-	2019-2	339				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710,				https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219,	/526
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	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, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9625, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8909, MSM8909W, MSM8909W, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8937, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, SDM8950, SDX20, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MDM9- 031219/527

Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Iot, Snapdragon om Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8053, APQ8096AU, APQ8053, APQ8096AU, APQ8053, MDM9206, MDM9206, MDM9607, MDM9615, MDM9625, MDM9615, MDM9650, MDM9650, MDM9655, MSM8909, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA645, SDM620, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDM20, SDX24, SDX25, SM6150, SM7150, SM8150, SM8250, Snapdragon, High_Med_2016, SXR1130, SXR2130    Improper   21-11-2019   Improper   21-11-2019   Information disclosure due   https://ww   O-QUA-	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Authenticati on				CVE ID : CVE-2019-2271		
Improper 21-11-2019 2.1 Information disclosure due https://ww O-QUA-	Authenticati	21-11-2019	10	allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9640, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8909, MSM8909W, MSM8909W, MSM8909W, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-	MDM9-
	Improper	21-11-2019	2.1	Information disclosure due	https://ww	O-QUA-

Weakness	Publish Date	CVSS	į.	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Restriction of Operations within the Bounds of a Memory Buffer			check buffer Snapo Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 MDM9 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM6 SDM8 Snapo CVE I	dragon_H 1130 <b>D : CVE-</b>	n the System the System to the System to the System to the Sonnective Consume and ustriated and the System to the	sDBG vity, er IOT, al IOT, Music, 009, 6, 6, 7, 1000,	w.qual m.com pany/y ct- securit lletins ber-20 bulleti	/com produ ty/bu /octo	MDM9- 031219	/529
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Weara APQ8	P modul out side it receive sage. Snapdradragon Indragon	e its bounges malforing Snapon Corsume andustria oT, Snapon Varagon APQ800 Q8053,	ndary ormed dragon mpute, er IOT, ol IOT, odragon Voice &	https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/530
	i			•	-		1			

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	/531
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID			Pat	ch	NCIIP	C ID	
			MDM9 MSM8 MSM8 MSM8 MSM8 QCS40 SDM4 SDM6 SDM6 SDM8 SM81 Snapo	lragon_I 1130, SX	DM9650 SM8909, SM8940, SM8996, MSM89 605, QM2 845, SDM 1450, SDM 1710, SDM 150, SM High_Me R2130	98, 215, M429, M630, M660, M845, 7150,				
Use After Free	21-11-2019	7.2	Use and cleaning missing for a fapplication composite of the consumer of the c	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130				//ww com /com produ ty/bu /octo 19- n	0-QUA- MDM9- 031219	/532
msm8909_fir	mware									
Loop with Unreachable Exit Condition ('Infinite	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute,				https:/ w.qual m.com pany/j ct- securit	com /com produ	0-QUA- MSM8- 031219	/533
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6			5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	i i	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Loop')			Snapo Snapo Mobil Music Weara APQ8 APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SC818 SDM6 SDM6 SDM6 SDM6 SDM8 SDX58 SM81 Snapo , SXR1	dragon Caragon Indragon Indrag	ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9607 DM9605 MDM9655 MB909, MSM8937, SM8937, SM8953, SM	l IOT, dragon dragon foice & 9, 8, 5, 40, 5, 40, 6, 40, M215, M450, M636, M710, X20, 150, d_2016	lletins ber-20 bulleti	19-		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &				https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/534
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
			Wears APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61 SM82	c, Snapdr ables in A 017, APC 096AU, A 9150, MI 9207C, M 9650, MS 3909, MS 3917, MS 3940, MS 3996, MS 3996, MS 3998, Nic 60, SDA 60, SDA 50, SM7	APQ800 Q8053, APQ809 DM9206 MDM960 SM8905 SM8909 SM8939, SM8939, SM8953, SM8953, SM8953, SM8953, SM8953, SM8956, SM8966, SM8966, SM8966, SM8966, SM8966, SM8966, SM8966, SM896	8, 5, 77, , , , , , , , , , , , , , , , ,				
Improper Validation of Array Index	21-11-2019	4.6	Out-o occur to imparray Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8	f-bounds in came proper ve index in Snapdra conics Co dragon In dragon Ve dragon Ve dragon We 009, APC 053, APC 098, MD 9207C, M 9640, MI 3905, MS 3909W, M 3920, MS 3940, MS 3996AU, 605, SDA	s access ra drive alidation Snapdr gon Coronsume adustria dobile, foice & Moreon March Mar	can r due n of agon nsumer ity, r IOT, l IOT, fusic, es in U, 7, 7,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/535
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDX20		
			CVE ID : CVE-2019-10503		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150  CVE ID: CVE-2019-2266	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/536
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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, APQ8096AU, APQ8098, MDM9150, MDM9205,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/537
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			MDM <sup>4</sup> MDM <sup>4</sup> MSM <sup>8</sup> MSM <sup>8</sup> MSM <sup>8</sup> MSM <sup>8</sup> MSM <sup>8</sup> Nicob QM21 SDA8 SDM <sup>4</sup> SDM <sup>6</sup> SDM <sup>7</sup> SDX20 SM61 SM82 Snapo , SXR1	9206, MI 9615, MI 9635M, I 9650, MS 3905, MS 3909W, I 3920, MS 3953, MS 3953, MS 3953, MS 36, SDM 45, SDM 45, SDM 45, SDM 50, SDM 50, SDX24 50, SM7 50, SM7 50, SM7	DM9625 MDM9655 MB909, MSM8910 SM8937, SM8940, SM8976, MSM89 2150, Qu 80X, SDA 429, SDA 1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	5, 40, 5, 17, 98, CS605, A660, M439, M632, M670, M850, 5,				
Improper Authenticati on	21-11-2019	10	allownersult allownersult bypas Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MDM MDM MD	of integrals MODER nessages into autoris of NAS dragon A dragon Colragon In dragon Io e, Snapdr ables in A 017, APO 096AU, A 9150, MI 9615, MI	M to acc s which a chentica in auto, compute consume ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9205 DM9607	ept any can tion  r IOT, l IOT, dragon oice &  9,  8, 5,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM3 MSM3 MSM3 MSM3 MSM3 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	9650, MI 8905, MS 8909W, I 8920, MS 8939, MS 8953, MS 8996AU, bar, QCM 15, SC818 45, SDM 450, SDM 710, SDM 0, SDX24 150, SM7 150, SM7 150, SX	5M8909, MSM8915 5M8940, 5M8976, MSM89 2150, Q 80X, SD 429, SD 1660, SD 1660, SD 1845, SD 150, SM	98, CS605, A660, M439, M632, M670, M850,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information lack check buffer Snape	mation description of the contraction of the contra	isclosur ress rang code. in auto, ompute onnection onsume dobile, foice & M Vired and APQ80 Q8053, SM8905 SM8917, SM8937, SM8937, SM8953, cobar, QM2	re due ge sDBG  vity, or IOT, l IOT, fusic,  CS404, 215,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	/539
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	l	Description	n & CVE	ID	Pat	ch	NCIIP	CID
			SDM6 SDM6 SDM8 Snapo , SXR1 CVE I	lragon_I l 130 <b>D : CVE-</b>	636, SD 710, SD High_Med <b>2019-2</b>	M660, M845, d_2016				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modulout side it receive tessage. Snapdradragon Idragon Idragon, MI 150, MI 150, MI 150, MI 150, SDM 15	its bour res malfo in Snapo gon Corr onsume dustria oT, Snap ragon V ragon APQ809 DM9607 DM9625 MDM9645 DM9655 SM8909, MSM891 SM8937, SM8940, SM8940, SM8940, SM8940, SM8940, SM8940, SM8940, SM8953, SM8940, SM8953, SM8940, SM8953, SM8940, SM8953, SM8940, SM8953, SM8940, SM8953,	ndary ormed dragon inpute, in IOT, dragon foice & 9, 8, 5, 40, 5, 47, 48, 48, 4660, 4439, 4660, 4439, 4650,	https:/w.qualm.company/jct-securitiletins.ber-20bulleti	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	/540
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0.1			<i>3</i> 7	-, 5	3.0	3,	, 3		3 10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			, SXR2	1130, SX	R2130					
			CVE I	D : CVE-	2019-2	303				
N/A	21-11-2019	7.2	copy to the Paramare frenviro Auto, Snapo	e invoking from fd of secure Inters be om non somment. Snapdradinagon Intergration Intergration Interpretation	or local louffer, eing popersecure in Snapersecure in Snaperse	ouffer oulated dragon inpute, vity, er IOT, l IOT,	https:/w.qualm.company/jct-securitiletins.ber-20bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/541
mdm9635m_f	firmware									
Loop with Unreachable	21-11-2019	5	While processing Attach Reject message, Valid exit				https:/ w.qual	•	O-QUA- MDM9-	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Exit Condition (Condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8917, MSM8909, MSM8917, MSM8909, MSM8917, MSM8920, MSM8933, MSM8976, MSM8933, MSM8976, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDM660, SDM645, SDM640, SDM645, SDM640, SDM640, SDM650, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDM20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon, High, Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA mcssages if network sends un-intended values in Snapdragon Auto, Security/bu leltins/octo	Weakness	Publish Date	cvss	[	Descriptio	n & CVE	ID	Pat	ch	NCIIF	PC ID
('Infinite Loop')  in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9655, MSM8909W, MSM8917, MSM890W, MSM8917, MSM890W, MSM8917, MSM890W, MSM8917, MSM899W, MSM8917, MSM890W, MSM8917, MSM890W, MSM8917, MSM896AU, MSM898, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM430, SDM636, SDM630, SDM50, SDM500, SDM630, SDM500, SDM510, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2335  Dut-of-bounds Read  Out-of-bounds Re	Exit			condi	tion is no	ot met		m.com	/com	031219	/542
Loop')  Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Ion. Snapdragon Ion. Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8900, MSM8933, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM630, SDM630, SDM630, SDM670, SDM710, SDM845, SDM820, SDS55, SM6150, SM7150, SM8150, SM8250, Snapdragon, High, Med_2016, SXR1130, SXR2130  CVE ID : CVE-2019-2335  Buffer over read can happen while parsing downlink session management 0TA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute,  DUt-of-bounds Read  Out-of-bounds	Condition				O		ite loop	pany/j	orodu		
Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8093, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9625, MDM9615, MDM9655, MSM8909, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA660, SDA645, SDM429, SDM439, SDM450, SDM630, SDM630, SDM630, SDM636, SDM630, SDM630, SDM636, SDM660, SDM710, SDM845, SDM8250, SDM660, SDM710, SDM845, SDM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130    Out-of-bounds Read	('Infinite			in Sna	pdragor	Auto,		ct-			
Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon ApQ8098, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9206, MDM9625, MDM9625, MDM9635M, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA645, SDM429, SDM439, SDM450, SDM439, SDM450, SDM632, SDM630, SDM632, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon, High_Med_2016, SXR1130, SXR2130    Out-of-bounds Read	Loop')			-	Ŭ	•					
Snapdragon   bulletin   Snapdragon   bulletin				-	Ŭ						
Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8909, MSM8909, MSM8909, MSM8917, MSM8900, MSM8917, MSM8900, MSM8953, MSM8900, MSM8953, MSM8976, MSM8996AU, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDM630, SDM500, SDM550, SM250, SDM550, SM8150, SM7150, SM8150, SM8250, SM8150, SM7150, SM8150, SM8250, Snapdragon-High_Med_2016 , SXR1130, SXR2130  CVE ID : CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Compute, lletins/octo  Out-of-bounds Read  OUT-of				•	•						
Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8933, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM670, SDM710, SDM845, SDM630, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2335  Dut-of-bounds Read  21-11-2019  Dut-of-bounds Read  Out-of-bounds Re				•	•	•	O	bulleti	n		
Wearables in APQ8009,					_	_	oice &				
APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDM845, SDM850, SDX20, SDM845, SDM850, SDX20, SDM845, SDM8250, Snapdragon_High_Med_2016 ,SXR1130, SXR2130 CVE ID: CVE-2019-2335  Out-of- bounds Read  21-11-2019  DUt-of- bounds Read  OUt-of- bo					•	•					
APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8997, MSM8976, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDM460, SDM630, SDM632, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon High, Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, lletins/octo  OUt-of-bounds Read  OUt-Scoring Scale						•	9,				
MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobarr, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM600, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, lletins/octo  OUt-of-bounds Read  OUt-of-bounds Read  OUt-of-bounds Read  OUt-of-bounds Read  OUt-of-bounds Read  OV Stories Sale				•		•	_				
MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 ,SXR1130, SXR2130 CVE ID : CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, letins/octo  OUt-of-bounds Read				_		•					
MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, lletins/octo  OUt-of-bounds Read  OUt-of-bounds Read  OUt-Storius Sole  OV Storius Sole  OV S					•		•				
MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM89020, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2335  Out-of- bounds Read  OUT-of- b					•		•				
MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM60, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, letins/octo  OUt-of-bounds Read					•		•				
MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID : CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA mcom/com pany/produ ct- bounds Read  21-11-2019  10  MSM8909, MSM8917, MSM8996AU, MSM8996AU, MSM8996AU, MSM8996AU, MSM8996AU, MSM8906, MSM8996AU, MSM8907, MSM8996AU, MSM8907, MSM8996AU, MSM8908, MSM8917, MSM8906, MSM8917, MSM8906, MSM8917, MSM8906, MSM8917, MSM8908, MSM8917, MSM8906, MSM8916, MSM8906, MSM8916, MSM8906, MSM8916, MSM8906, MSM8916, MSM8908, MSM8917, MSM8906, MSM8916, MSM8906, MSM896, MSM8906, MSM896, MSM8906, MSM896, MSM8906, MSM896, MSM8906, MSM8916, MSM8906, MSM896, MSM8906, MSM896, MSM8906, MSM896, MSM8906,					•		•				
MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID : CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, lletins/octo  CV Scoring Scale  MSM8909W, MSM8937, MSM8937, MSM8996AU, MSM8996AU, MSM8996AU, MSM8996AU, MSM8996AU, MSM8996AU, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA640, SDM615, SDM630, SDM632, SDM636, SDM670, SDM710, SDM710, SDM8150, SM8250, SM8150, SM8250, SM8150, SM8250, SM8150, SM7150, SM8150, SM8250, SM8150, SM220, SM8150, SM220, SM8150, SM220, SM9429, SDM636, SM8150, SM220, SM9429, SDM636, SM8996AU, MSM8998, Nicobar, QCM215, SC8180X, SDA660, SDA645, SDM630, SDM632, SDM630, SDM636, SDM630, SDM6312, SDM630,											
MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, lletins/octo  CV Scoring Scale  MSM8920, MSM8993, MSM8996AU, MSM8996AU, MSM8996AU, MSM8996AU, MSM8996, MSM8996AU, MSM8996, MSM8996AU, MSM8996, MSM8996AU, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM450, SDM450, SM8150, SM8250, Snapdragon Auto, Snapdragon Compute, lletins/octo											
MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA mcom/com pany/produ ct- messages if network sends un-intended values in Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, letins/octo  OCVScoring Scale					•		•				
MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA m.com/com pany/produ un-intended values in Snapdragon Auto, Snapdragon Auto, Snapdragon Compute,  OUt-Scoring Scale					-	•					
MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA m.com/com pany/produ un-intended values in Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, lletins/octo  OUt-of-bounds Read  OUT-OF-DOUGH MDM9- O31219/543											
Out-of-bounds Read  Out-of							10,				
SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Spansor Comp							M215.				
SDM429, SDM439, SDM450, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2335  Buffer over read can happen while parsing downlink session management OTA mcom/com messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, SDM439, SDM450, SDM439, S				-	_	_					
Out-of-bounds Read  Out-of					•		•				
Out-of-bounds Read  Out-of					•	•	•				
Out-of-bounds Read  Out-of					•	•	•				
Out-of-bounds Read  Out-of				SDM8	45, SDM	850, SD	X20,				
Out-of-bounds Read  Out-of				SDX5	5, SM615	50, SM71	150,				
Out-of-bounds Read  21-11-2019  Out-of-bounds Read  Out-of-bounds				SM81	50, SM82	250,					
Out-of-bounds Read  Out-of				Snapd	lragon_H	ligh_Med	d_2016				
Out-of-bounds Read  21-11-2019  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute,  CV Scoring Scale  Buffer over read can happen whiteps://ww w.qualcom m.com/com pany/produ ct- 0-QUA-MDM9- 031219/543											
Out-of-bounds Read  21-11-2019  10  while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute,  W.qualcom m.com/com pany/produ ct- 031219/543  MDM9-031219/543				CVE I	D : CVE-	2019-2	335				
Out-of-bounds Read  21-11-2019  10  while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute,  W.qualcom m.com/com pany/produ ct- 031219/543  MDM9-031219/543				Buffer	over re	ad can h	appen	https:/	//ww		
Out-of-bounds Read  21-11-2019  10  session management OTA m.com/com pany/produ ct- 031219/543  Snapdragon Auto, Snapdragon Compute, lletins/octo								• •	•		
bounds Read  21-11-2019  10  messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute,  CV Scoring Scale  21-11-2019  10  messages if network sends un-intended values in Snapdragon Compute,  MDM9- 031219/543	Out of				_			_		O-QUA-	
un-intended values in Snapdragon Auto, Snapdragon Compute, OV Scoring Scale		21-11-2019	10		_				•	MDM9-	
Snapdragon Compute, lletins/octo	Douling Read				_				-	031219	/543
CV Scoring Scale				Snapd	lragon A	uto,		securit	y/bu		
CV Scoring Scale 0.1 1.2 2.3 3.4 4.5 5.6 6.7 7.9 9.0 0.10				Snapdragon Compute,							
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	_	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIF	C ID
			Snapo Snapo Snapo Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	dragon C dragon In dragon Id e, Snapdr ables in A 017, APC 096AU, A 9150, MI 9635M, I 9635M, I 9635M, I 9635M, I 9635M, I 9635M, I 9639, MS 3909W, I 3909W, I 390W, I 390W, I 390W, I 390W, I 390W, I 390	onsume adustria oT, Snap tragon Vagon APQ800 Q8053, APQ809 DM9625 MDM9625 MDM9655 MB9676, MSM8937, SM8940, SM8976, ASDA 429, SDA	r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, 40, 6, M439, M632, M670, M850, 5,	ber-20 bulleti			
Improper Authenticati on	21-11-2019	10	allows NAS n result bypas Snapo Snapo Snapo Snapo	of integriss MODENtessages into autors of NAS dragon Caragon Caragon Indragon Idragon	M to accombined to accombine the second to accombine t	ept any can tion , or IOT, l IOT,	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	/com /com produ ty/bu /octo	O-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	NCIIF	PCID					
			Mobil Music Wears APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	e, Snapdr ables in 2 017, APO 096AU, 2 9150, MI 9206, MI 9635M, I 9635M, I 9635M, I 3905, MS 3909W, I 3920, MS 3939, MS 3939, MS 3953, MS 3953, MS 3953, MS 3953, MS 3053, SDM 45, SDM 45, SDM 450, SDM 450, SDM 50, SDM 50, SDM	Tagon V Tagon V APQ800 Q8053, APQ809 DM9607 DM9625 MDM9655 MSM8937, MSM8937, MSM8940, MSM8940, MSM8940, MSM8940, MSM8955, MSM8956, MSM8956, MSM8956, MSM8940, MSM8955, MSM8940, MSM8940, MSM8956, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8955, MSM8940	oice & 9, 8, 5, 7, 5, 40, 5, 7, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Weara APQ8	P modul out side it receive essage. Snapdradragon Idragon Idra	its bounges malfoling Snapon Corsume andustria oT, Snapon Vagon APQ800 Q8053,	ndary ormed dragon mpute, or IOT, dragon oice &	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 6-7 7-8							9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303		
qca9980_firm	iware			,	
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	0-QUA-QCA9- 031219/546

3-4

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
		MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266			
sdm429_firm	ware		0.2.2.0.2.2.0.2.2.0.0		
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	0-QUA-SDM4- 031219/547

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			, SXR1	130, SX	R2130					
			CVE I	D : CVE-	2019-2	335				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated to will be modifi		ce lock verently the memory ds to out in Snape agon Core consume industria oT, Snape lragon Veragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905	which  Tpy  t of dragon nsumer ity, or IOT, l IOT, odragon Toice &  9,  8, 7C, 0, , 89, AU, CS605, 845, M630, M660, X20, 150,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
				<b>D : CVE-</b> r over re			https:/	//ww		
Out-of- bounds Read	21-11-2019	10	while session messa un-int Snapo Snapo	parsing on manag nges if ne tended v dragon A dragon C	downlir gement ( etwork s values in auto, compute	nk OTA sends	w.qual m.com pany/j ct- securit lletins, ber-20	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Mobil Music Wears APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	dragon Indragon Indragon Idee, Snapdragon Idee, Snapdragoles in Applementation of the Idea	oT, Snap ragon V ragon APQ800 Q8053, APQ809 DM9607 DM9625 MDM9655 GM8909, MSM891 GM8937, GM8940, GM8976, MSM89 2150, Qu 30X, SDA 429, SDI 6630, SDA 429, SDI 6660, SD 6660, SD 6845, SD 6845, SD 6845, SD 6845, SD 6845, SD	dragon oice & 9, 8, 40, 5, 40, 6, M439, M632, M670, M850, 7, 8150, d_2016	bulleti	n		
Improper Authenticati on	21-11-2019	10	allow NAS result bypas Snapo Snapo Snapo Snapo Snapo	of integra s MODEI messages into aut ss of NAS dragon A dragon C dragon I dragon I dragon I dragon I e, Snapd	M to accombined to the second of the second	ept any can tion r IOT, l IOT, dragon	https:/ w.qual m.com pany/p ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIF	C ID
			Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	c, Snapdrables in 2017, APC 096AU, 29150, MS 9635M, 29650, MS 3909W, 18920, MS 3996AU, 250, SDM 250, SDM 250, SDM 250, SM7 50, dragon_H 1130, SX D: CVE-	APQ800 Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 GM8909, MSM8937, GM8976, MSM8976, MSM89, Q150, Q0 80X, SDA 429, SDA 42	8, 5, 40, 5, 40, 5, 47, 27, 28, 27, 4660, 4632, 4670, 4670, 4670, 8150,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape Snape Snape Snape Snape Snape Snape Snape Infras	mation d k of addi done or s in SDI dragon C dragon C dragon I dragon W dragon V dragon V structure orking in	ress range the System code. in Auto, compute connection consume ndustria Mobile, voice & M Vired e and	ge DBG vity, r IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>4</sup> MSM8 MSM8 MSM8 QCS44 SDA6 SDM4 SDM6 SDM6 SDM8 Snapo	lragon_H	5M8905 5M8917, 5M8937, 5M8953, cobar, Q 05, QM2 645, SD 450, SD 710, SD	CS404, 215, 4429, M630, M660, M845,				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear; APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	P modul out side it receiv essage. it sapdra dragon Caragon Ir dragon Ir dragon, MI 9650, MI 965	e may active may active malforms malforms malforms malforms may active may ac	ccess idary ormed dragon inpute, r IOT, dragon oice &  9,  8,  7,  40,  7,  77,	https:/w.qualm.com pany/jct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-3 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	1	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	45, SDM 50, SDM 36, SDM 10, SDM 0, SDX24 50, SM7 50, dragon_H 1130, SX <b>D: CVE</b> -	1630, SD 1660, SD 1845, SD 1, SDX55 150, SM High_Me R2130	M632, M670, M850, 8150, d_2016				
N/A	21-11-2019	7.2	copy to the Paramare from Environment of Snapor Sna	e invoking from fd of a secure of the comment. Snapdragon of the comment of the c	or local lebuffer, eing popsecure in Snapegon Consumendustria Mobile, Voice & More and a APQ80 Q8053, Q8096A Q805, QM9150, SM8909 Q805, SM8900 Q805, SM8900 Q805, SM8900 Q805, SM8900 Q805, SM89	ouffer oulated dragon npute, vity, er IOT, l IOT, U, 09, U, 5, 0, 4, 98, 215, M429, M630, M660, M845,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-3 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			, SXR1	50, lragon_H 130, SX <b>D : CVE-</b>	R2130					
Out-of- bounds Read	21-11-2019	2.1	Trustimemo result Snapo	ecure Kozone to ozone diragon oz	do an ar which was in auto, connectionsume ndustrial Mobile, Moice & Movined e and n APQ80 Q8096, IPQ8074 SM8940, SM8940, QCA808 429, SDM 1632, High_Me	bitrary vill vity, r IOT, l IOT, lusic, 17, 4, 4, 1439, d_2016	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-: 031219	
sdm632_firm	ware		•							
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi result in Sna Snapo Snapo Snapo Snapo Mobil Musio	process messag tion is no ing into pdragon C dragon I dragon I	ge, Valid ot met an infin n Auto, compute consume ndustria oT, Snap lragon V	exit ite loop , er IOT, l IOT, dragon oice &	https://w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7 7-8		8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SDM4 SDM6 SDM6 SDM6 SDM6 SDM8 SDX58 SM81 Snapo	017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MS 3905, MS 3909W, I 3920, MS 3976, MS 3976, MS 3976, MS 3976, MS 3976, MS 30X, SDM 50, SDM 545, SDM 545, SDM 545, SDM 545, SM61S 1130, SX D: CVE-	APQ809 DM9205 DM9607 DM9625 MDM9655 MSM8909, MSM8915 SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8975	5, 7, 6, 40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150,				
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack o will b modification stater bound Auto, Electr Snapo Snapo Mobil Music Wears APQ8 APQ8	condition of resour e concur fied in the ment lead d access Snapdra conics Co dragon I dragon	ce lock werently the memorals to our in Snaper ingon Corr onnective consume industria oT, Snaper dragon V ragon APQ800 Q8053, APQ809	which  py t of dragon nsumer ity, or IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>4</sup> MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX2 SM81	9607, MI 9650, MS 3909W, N 3953, MS 3998, Nic 605, QCS 5, SDA6 29, SDM 32, SDM 10, SDM 4, SM615 50	5M8905 MSM8936, cobar, 5405, Q0 60, SDA 439, SD 636, SD 845, SD	, 39, AU, CS605, 845, M630, M660, X20,				
Out-of- bounds Read	21-11-2019	10	while session messar un-information of the session messar un-information of the session of the s	r over reparsing on manages if netended valuages if netended valuages if netended valuages in Aluages in Aluag	downlingement of tworks alues in uto, ompute onsume ndustria oT, Snap ragon APQ800 Q8053, APQ809 QM9625 QM9625 QM9625 QM9625 QM9655 QM9655 QM9655 QM9655 QM8937, QM893	nk OTA ends  r IOT, l IOT, dragon oice &  9,  8,  7,  7,  77,  98,  CS605,	https://w.qualm.com pany/jct-securit lletins/ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

SDA845, SDM429, SDM439, SDM430, SDM450, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	Weakness	Publish Date	cvss		Description	n & CVE	Pat	ch	NCIIP	CID	
allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8098, Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8098, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9615, MDM9615, MDM9615, MDM9655, MDM9615, MDM9655, MDM9655, MSM8905, MSM8909, MSM8917, MSM8905, MSM8909, MSM8917, MSM8939, MSM8918, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM630, SDM630				SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	50, SDM 36, SDM 10, SDX24 50, SM7 50, dragon_H	1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	M632, M670, M850, , 8150, d_2016				
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Authenticati	21-11-2019	10	allow NAS result bypas Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4	s MODEI nessages into aut s of NAS dragon A dragon G dragon Id dra	M to accion which of the consumer of the consu	ept any can tion  r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 6, 40, 6, 4660, M439, M632, M632,	w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	•	
	CV Scoring Scal (CVSS)	e <u>0-1</u>	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	1	Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			SDX2 SM61 SM82 Snapo , SXR1	10, SDM 0, SDX24 50, SM7 50, dragon_H 1130, SX <b>D : CVE-</b>	l, SDX55 150, SM High_Me R2130	d_2016				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information lack check buffer Snaper SNAP	mation days of addition of addition of addition of addition of a diragon of a diragon, of a dirag	isclosur ress rang the Sys code. in auto, compute connective consume ndustria Mobile, Vired and APQ80 Q8053, SM8905 SM8917, SM8937, SM8937, SM8953, cobar, Q M250, QM2 SM8953, Cobar, Q M250, SDM M250, SDM M2	re due ge sDBG  , vity, er IOT, l IOT, l IOT, Music, CS404, 215, M429, M630, M660, M845, d_2016	https:/w.qualm.company/jct-securitelletinsber-20bulletins	com /com produ ty/bu /octo	0-QUA-3 031219	
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon				https:/ w.qual m.com pany/	lcom l/com	0-QUA-:	
CV Scoring Scale (CVSS)	e 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapd Snapd Snapd Mobil- Music Weara APQ86 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA84 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapd , SXR1	Snapdra lragon Ic lragon Ic lragon Ic e, Snapdra bles in 2 017, APO 096AU, 2 9150, MI 9635M, Ic	onsume industria of, Snap ragon Vagon APQ800 DM9605 DM9605 DM9605 DM9655 BM8909, MSM891 BM8937, SM8940, SM8940, SM8940, SM8956, SD E660, S	r IOT, l IOT, dragon oice & 9, 8, 40, 5, 7, 7, 28, CS605, M439, M670, M632, M670, M850, ,	ct- securit lletins, ber-20 bulleti	octo 19-		
N/A	21-11-2019	7.2	copy for to the Param are from environments Auto,	invoking from fd of secure lands because the secure lands because the secure lands and secure lands are lands and secure land	or local bouffer, eing pop secure in Snapo gon Cor onnectiv	ouffer oulated dragon npute, vity,	https://w.qual m.com pany/j ct- securit lletins/ ber-20	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3		4-5	5-6	6-7	7-8	8-9	

Snapdragon Industrial IOT, Snapdragon Wobile, Snapdragon Wobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ80963, APQ8096AU, APQ8096AU, APQ8096AU, APQ8096AU, APQ8096, MDM9205, MDM9205, MDM9206, MDM9650, MSM8907, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8937, MSM8940, MSM8953, MSM896AU, MSM8953, MSM8998, QCS404, QCS065, QM215, SDA660, SDM630, SDM632, SDM630, SDM630, SDM632, SDM630, SDM650, SM150, SM8150, Snapdragon High_Med_2016, SXR1130, SXR2130    CVE ID : CVE-2019-2315	Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Out-of-bounds Read  Out-of-Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074,  O-QUA-SDM6-031219/562				Snapo Snapo Snapo Infras Netwo APQ8 APQ8 APQ8 MDM' MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM6 SDM8 SM81 Snapo , SXR1	dragon Maragon Valragon Valragon Valragon Valragon Valragon Valragon, APO 1096, APO 1098, MD 1096, MS 1096, MS 1096, MS 1096, SDA 1096,	Mobile, Foice & Mobile, Foice	Music,  09,  U,  98,  215,  M429,  M630,  M660,  M845,  7150,  d_2016	bulleti	n		
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		21-11-2019	2.1	Trusti memo result Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo	zone to o ory read into DO dragon A dragon I dragon W dragon V dragon V structure orking ir 053, APO	do an ari which w S in uto, onnectiv onsume ndustria fobile, foice & M Vired and APQ80 Q8096,	bitrary vill vity, r IOT, l IOT, fusic,	w.qual m.com pany/i ct- securit lletins ber-20	com /com produ ty/bu /octo	=	
	_	e <u>0-1</u>	1-2					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, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318		
msm8917_fir	mware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA- MSM8- 031219/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130		
			CVE ID: CVE-2019-2335		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8937, MSM8938, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130  CVE ID: CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MSM8- 031219/564
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer	https://ww w.qualcom m.com/com pany/produ ct-	O-QUA- MSM8- 031219/565
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	tch	NCIIP	C ID
			Snapd Snapd Snapd Snapd APQ80 APQ80 APQ80 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDX20		onsumendustria dobile, doice & Magentable (28017, (28096A) (28096A	Fr IOT, I IOT, I IOT, Music, es in U, 07, 0, 17, 18, 198, 0M450, M660,	securitiletins ber-20 bulleti	/octo )19-		
Out-of- bounds Read	21-11-2019	10	Buffer while session messa un-intended Snaped Snaped Snaped Mobile Music Wears APQ86 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM	D: CVE- rover re parsing n manag ges if ne tended v lragon C lragon I lragon I lragon I lragon I lragon I logon I logo	ad can had can	nappen nk OTA sends or IOT, l IOT, odragon oice & o o o o o o o o o o o o o o o o o o o	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- MSM8- 031219	/566
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX20 SM61 SM82 Snapo	3909W, I 3920, MS 3939, MS 3953, MS 3996AU, ar, QCM 55, SC818 45, SDM 50, SDM 50, SDM 50, SM7 50, SM7 50, SM7	5M8937, 5M8940, 5M8976, MSM89 2150, Q0 80X, SDA 429, SDI 6630, SD 6660, SD 6845, SD 845, SD 150, SM	98, CS605, A660, M439, M632, M670, M850, ,				
Improper Authenticati on	21-11-2019	10	Lack of allow NAS in result bypas Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MSM8 MSM8	of integral of int	ity check M to accombined to chentical in auto, ompute onsume ot, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9625 MDM9645 SM8909, MSM891	ept any can tion  r IOT, l IOT, dragon oice &  9,  8,  7,  40,  5,	https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/567
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)										

Weakness	Publish Date	cvss	1	Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			MSM8 Nicob QM21 SDA84 SDM4 SDM7 SDX20 SM61 SM82 Snapd	lragon_H l 130, SXI	MSM89 2150, Qu 80X, SDA 429, SDI 1630, SD 1660, SD 1845, SD 150, SMI High_Med R2130	98, CS605, A660, M439, M632, M670, M850, 5, 8150,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,				https:/ w.qual m.com pany/i ct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA- MSM8- 031219	/568
				850, dragon_H	liah Ma	d 2014				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130		
			CVE ID : CVE-2019-2295		
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM8953, MSM8976, MSM8953, MSM8976, MSM8953, MSM8976, MSM8953, SDM450, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM63	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/569
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer	https://ww w.qualcom	O-QUA- MSM8-
CV Cooring Co-1			copy from to or local buller	w.quarcom	1-101-10
CV Scoring Scal (CVSS)	e 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ807, APQ8096AU, APQ8096, APQ8096AU, APQ8096, MDM9205, MDM9206, MDM9205, MDM9206, MDM9205, MDM9206, MDM9205, MSM8909, MSM8917, MSM890	Weakness	Publish Date	CVSS		escriptio	n & CVE	ID	Pat	ch	NCIIF	PC ID
are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Noise & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8900, MSM8917, MSM8900, MSM8917, MSM8940, MSM8953, MSM8906, MSM8996AU, MSM8996, MSM8996AU, MSM8996, MSM8996AU, MSM8996, MSM8996AU, MSM8998, QC5404, QC5605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon High_Med_2016 ,SXR1130, SXR2130 CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Consumer IOT, Snapdragon Industrial IOT,  OUt-of- Snapdragon Industrial IOT,  OUT-STATUS AND				to the	secure l	ouffer,		m.com	/com	031219	/570
environment. in Snapdragon						• • •	ulated	pany/p	orodu		
Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8093, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8900, MSM8917, MSM8990, MSM8937, MSM8990, MSM8937, MSM8996, MSM8937, MSM8998, QC\$404, QC\$605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  OUt-of- born Selection Selection ber-2019-				are fro	m non s	secure		ct-			
Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8998, QC\$404, QC\$605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Sn						•	O				
Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096, APQ8096, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8906, MSM8905, MSM8909, MSM8917, MSM8996, MSM8996, MSM8917, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, MSM8963, SDM636, SDM636, SDM640, SDM670, SDM450, SDM630, SDM630, SDM632, SDM636, SDM636, SDM600, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016				•	•	U	•	•			
Snapdragon Industrial IOT,   Snapdragon Mobile,   Snapdragon Woice & Music,   Snapdragon Wired   Infrastructure and   Networking in APQ8009,   APQ8017, APQ8053,   APQ8096, APQ8096AU,   APQ8098, MDM9150,   MDM9205, MDM9206,   MDM9607, MDM9650,   MSM8905, MSM8909,   MSM8905, MSM8909,   MSM8917, MSM8909,   MSM8937, MSM8909,   MSM8937, MSM8940,   MSM8953, MSM8996,   MSM8953, MSM8996,   MSM8953, MSM8996,   MSM8953, MSM8996,   MSM8953, MSM8996,   MSM8953, MSM8909,   MSM8953, MSM8909,   MSM8953, MSM8909,   MSM8953, MSM8906,   MSM8953, MSM8906,   MSM8953, MSM8906,   MSM89064U, MSM8998,   QC\$404, QC\$605, QM215,   SDA660, SDM630, SDM632, SDM636, SDM660,   SDM630, SDM632, SDM636, SDM660,   SDM670, SDM710, SDM845,   SDM850, SM6150, SM7150,   SM8150,   Snapdragon High_Med_2016   , SXR1130, SXR2130   CVE ID: CVE-2019-2315   Non Secure Kernel can cause   Trustzone to do an arbitrary   memory read which will   result into DOS in   Snapdragon Auto,   Snapdragon Consciuity,   Snapdragon Consciuity											
Snapdragon Mobile,   Snapdragon Voice & Music,   Snapdragon Wired   Infrastructure and   Networking in APQ8009,   APQ8017, APQ8053,   APQ8096, APQ8096AU,   APQ8098, MDM9205, MDM9206,   MDM9205, MDM9206,   MDM9205, MSM8909,   MSM8917, MSM8909,   MSM8917, MSM8920,   MSM8937, MSM8940,   MSM8953, MSM8996,   MSM8953, MSM8996,   MSM8954, MSM8996,   MSM8954, SDM429, SDM439, SDM450, SDM630, SDM632, SDM632, SDM630, SDM632, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM845, SDM850, SM6150, SM7150,   SM8150, Snapdragon_High_Med_2016				_	•			bulleti	n		
Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9205, MDM9206, MDM9607, MDM9607, MSM8909, MSM8917, MSM8909, MSM8917, MSM8909, MSM8917, MSM8909, MSM8917, MSM8996, MSM89853, MSM8996, MSM8937, MSM8940, MSM8953, MSM8996, MSM8950, SM6150, SDM429, SDM439, SDM450, SDM630, SDM632, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM6150, SM7150, SM8150, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130   CVE ID : CVE-2019-2315				_	_		l IOT,				
Snapdragon Wired   Infrastructure and   Networking in APQ8009,   APQ8017, APQ8098, APQ8096, APQ8096AU,   APQ8098, MDM9150,   MDM9205, MDM9206,   MDM9205, MDM9206,   MDM9607, MDM9650,   MSM8905, MSM8909,   MSM8917, MSM8920,   MSM8917, MSM8920,   MSM8937, MSM8996,   MSM8996,   MSM8996AU, MSM8996,   MSM8996AU, MSM8998,   QCS404, QCS605, QM215,   SDA660, SDA845, SDM429,   SDM439, SDM450, SDM630,   SDM632, SDM632, SDM630,   SDM632, SDM636, SDM660,   SDM670, SDM710, SDM845,   SDM850, SM6150, SM7150,   SM8150,   Snapdragon_High_Med_2016   , SXR1130, SXR2130   CVE ID : CVE-2019-2315				_	•						
Infrastructure and   Networking in APQ8009, APQ8017, APQ8017, APQ8053, APQ8096, APQ8096, APQ8096, APQ8096, APQ8096, APQ8096, APQ8098, MDM9150, MDM9205, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8996, MSM8993, MSM8996, MSM8993, MSM8996, MSM8993, MSM8996, MSM8993, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM60, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8150, SM8150, SM2130    CVE ID : CVE-2019-2315				_	•		Iusic,				
Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8909, MSM8917, MSM8920, MSM8937, MSM8996, MSM8937, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, MSM8996, MSM8998, QCS404, QCS605, QM215, SDA660, SDA645, SDM429, SDM439, SDM450, SDM630, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID : CVE-2019-2315  Out-of-bounds Read  21-11-2019  2.1   Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, ber-2019-				_	•						
APQ8017, APQ8053,											
APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM629, SDM439, SDM630, SDM630, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, ber-2019-					•	•	09,				
APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8937, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, CV Scoting Scale  APQ8098, MDM9206, MDM9205, MDM9206, MSM8905, MSM8909, MSM8990, MSM8998, QCS404, QCS605, QM215, SDM630, SDM630, SDM642, SDM630, SDM642, SDM640, SDM642, SDM640, SDM642, SDM640, SDM642, SDM640, SM742, SDM640, SM				_		•					
MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT,  CV Scoting Stale  MMDM9205, MDM9650, MSM8905, MSM8909, MSM8996, MSM8996, MSM8998, QCS404, QCS605, QM215, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM640, SDM				_		•					
MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon In				_ ~	•	-					
MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT,  MSM8-031219/571											
MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  DVS. Scoring Scale  MSM8937, MSM8996, MSM8960, SDM610, SDM620, SM8150, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon											
MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, SNAP STAN STAN SAME  O'V Scoring Scale  O'V Scoring Scale					•	•					
MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Indu					•	•					
MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Security Scale					•	•					
Out-of-bounds Read  Out-of											
Out-of-bounds Read  Out-of					•		•				
Out-of-bounds Read  Out-of				_							
SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT,  SDM845, SDM845, SDM850, SM6150, SM7150, SM8150, SNAP130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, SNAPOROUM SECURITY SECURIT											
Out-of-bounds Read  Out-of				SDM6	32, SDM	636, SD	M660,				
Out-of-bounds Read  21-11-2019  SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT,  Snapdragon Industrial IOT,  Snapdragon Scale  SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  Lettos:  Very Scoring Scale  Snapdragon Industrial IOT, Snapdragon Industrial				SDM6	70, SDM	710, SD	M845,				
Out-of-bounds Read  21-11-2019  Out-of-bounds Read  Out-of-bounds				SDM8	50, SM6	150, SM	7150,				
Out-of-bounds Read  Out-of				SM81	50,						
Out-of-bounds Read  21-11-2019  2.1  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT,  CV Scoring Scale  Non Secure Kernel can cause https://ww w.qualcom mm.com/com pany/produ ct-security/bu lletins/octo ber-2019-				Snapd	ragon_F	ligh_Me	d_2016				
Out-of-bounds Read  Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT,  Out-of-wu-depth with will will will will microm/com pany/produ ct-security/bu security/bu lletins/octo ber-2019-				, SXR1	130, SX	R2130					
Out-of-bounds Read  21-11-2019  2.1  Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, ber-2019-  CV Scoring Scale  Trustzone to do an arbitrary w.qualcom m.com/com pany/produ ct- security/bu Snapdragon Connectivity, Snapdragon Consumer IOT, ber-2019-				CVE II	D : CVE-	2019-2	315				
Out-of-bounds Read  Out-of-commemory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Out-of-commemory read which will result into DOS in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Out-of-commemory read which will result into DOS in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Out-of-commemory read which will result into DOS in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT,				Non S	ecure Ke	ernel car	n cause	https:/	//ww		
Out-of-bounds Read  21-11-2019  2.1 result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Scale  CV Scoring Scale  21-11-2019  2.1 result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon I				Trustz	zone to c	lo an arl	bitrary	w.qual	com		
bounds Read  21-11-2019  21-11				memo	ry read	which w	vill	m.com	/com	O-011A-	
Snapdragon Auto, ct- 031219/571 Snapdragon Connectivity, security/bu Snapdragon Consumer IOT, Snapdragon Industrial IOT, ber-2019-		21-11-2019	2.1	result	into DO	S in				_	
Snapdragon Connectivity, security/bu Snapdragon Consumer IOT, lletins/octo Snapdragon Industrial IOT, ber-2019-	bounds Read		211	Snapd	ragon A	uto,		ct-			)/571
Snapdragon Industrial IOT, ber-2019-				Snapd	ragon C	onnectiv	vity,	securit	y/bu	001217	, 0, 1
CV Scoring Scale				Snapd	ragon C	onsume	lletins	octo/			
CV Scoring Scale 0.1 1.2 2.3 2.4 4.5 5.6 6.7 7.9 9.0 0.40				Snapd	ragon Ir	ndustria	l IOT,	ber-20	19-		
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	_	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318	bulletin	
msm8920_fir	mware		0.2.2.0.2.2020		
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MSM8- 031219/572

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

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, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/573

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130		
			CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM896AU, MSM8953, MSM896AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/574
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA- MSM8- 031219/575
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Desc	cription & CV	'E ID	Pat	ch	NCIIP	C ID
			APQ8017 APQ8096 MDM915 MDM920 MDM961 MDM963 MDM965 MSM890 MSM890 MSM892 MSM893 MSM895 MSM895 Nicobar, QM215, S SDA845, SDM450, SDM636, SDM710, SDX20, S SM6150, SM8250, Snapdrag , SXR1136						
Improper Authenticati on	21-11-2019	10	CVE ID: CVE-2019-2271  Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205,			https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/576
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> Nicob QM21 SDA8 SDM <sup>o</sup>	9206, MI 9615, MI 9635M, I 9650, MI 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3953, MS 3953, MS 36, SDM 45, SC818 45, SDM 45, SDM 450, SDM 50, SDX24 50, SM7 50, SM7 50, SM7	DM9625 MDM9655 MB909, MSM8915 SM8937, SM8976, MSM89 2150, Q0 30X, SDA 429, SDA 429, SDA 5660, SD 6660, SD 6845, SD	5, 40, 5, 7, 98, CS605, A660, M439, M632, M670, M850, ,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape Snape Snape Snape Snape Snape Snape Snape Snape Mode Mode MSM8	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,				//ww lcom produ ty/bu /octo )19- n	0-QUA- MSM8- 031219	/577
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	Pat	ch	NCIIP	C ID	
			QCS4 SDA6 SDM6 SDM6 SDM6 SDM8 Snapo	lragon_F	505, QM: 345, SDN 1450, SD 1636, SD 1710, SD High_Me	215, M429, M630, M660, M845, d_2016				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	P modulout side it received assage. Snapdra dragon Idragon Idr	its bounces malfolin Snapolingon Consumeration, Snapolingon Vagon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9655 MB9655 MB9655 MB9655 MB976, MSM8937, SM8940, SD808, SD	ndary ormed dragon mpute, er IOT, el IOT, edragon foice & e9, es, es, es, es, es, es, es, es, es, es	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	/578
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	21-11-2019	7.2	SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2303  While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9206, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8953, MSM8996, MSM8996, MSM8996AU, MSM8996, MSM8996AU, MSM8996, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MSM8- 031219/579
			MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	bulletin	

4-5

6-7

5-6

7-8

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MSM8- 031219/580
msm8937_fir	mware				,
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/581

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>o</sup> MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9615, MI 9635M, I 9635M, I 9650, MS 3905, MS 3909W, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDM 30X, SDM 30, SDM 30, SDM 35, SM615 1130, SXI	MDM96-55 M8909, MSM8915 M8953, M8953, M896-605, Q M660, SD M632, SD M632, SD M630, S	40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150,				
Use After Free	21-11-2019	2.1	Use and daem static freed in Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MSM8 MSM8	ter free free fon shutd object in from a napdragon Caragon Caragon Indragon	issue in lown du stance in Auto, ompute onnectionsume ndustria oT, Snap ragon APQ800 Q8053, APQ809 DM9206 SM8905 SM8905 SM8905 SM8905 SM8920,	Xtra e to getting places  vity, or IOT, l IOT, dragon oice &  9,  8,  7,  W,	https:/ w.qual m.com pany/i ct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA- MSM8- 031219	/582
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			MSM8 MSM8 SDA6 SDM6 SDM8 SM61	3940, MS 3996, MS 3998, Nio 60, SDA 60, SDM 45, SDX 50, SM7	5M8996, cobar, Q 345, SDN 1670, SD 20, SDX 150, SM	AU, CS605, 4450, M710, 24,				
			CVE I	D : CVE-	2019-1	0490				
Improper Validation of Array Index	21-11-2019	4.6	occur to imparray Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM' MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDX2	f-boundin came proper vindex in Snapdra conics Codragon Indragon Indragon Vinagon Vina	ra drive alidation Snapdr igon Cor onnectiv consume idustria Mobile, Yoice & M Vearable Q8017, Q8096A M9206, MDM9650 DM9650 DM9650 SM8909, MSM891 SM8937, SM8933, MSM89 A660, SI	r due n of agon nsumer ity, r IOT, l IOT, U, O7, O7, O7, Music, es in U, Music, es in Mu	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/583
Out-of- bounds Read	21-11-2019	10	while sessic messa un-in	r over re parsing on manag nges if ne tended v	downlir gement ( etwork s values in	nk OTA sends	https://w.qual m.com pany/j ct- securit	com /com produ	0-QUA- MSM8- 031219	/584
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDM6 SDM7 SDM2 SM61 SM82 Snapo Snapo	dragon C dragon In dragon In dragon In dragon Io e, Snapdr ables in Io 017, APO 096AU, Io 9615, MI 9615, MI 9635M, Io 9650, MI 3905, MS 3905, SDM 450, SDM	compute on sume industria of, Snap dragon Vagon APQ800 Q8053, APQ809 DM9605 DM8906 DM9605 DM8906 DM8906 DM9605 DM9600 DM9	r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, M439, M632, M670, M850, 8150,	lletins, ber-20 bulleti	19-		
Improper Authenticati on	21-11-2019	10	allow NAS n result bypas Snapo Snapo Snapo	of integra s MODEI nessages t into aut ss of NAS dragon A dragon C dragon I	M to accommend to	ept any can tion , r IOT,	https://w.qual m.com pany/j ct- securit lletins/ ber-20	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ſ	Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	lragon Ide, Snapdon, Snapdon, Apoles in Apoles	lragon V ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MB9676, MSM8937, SM8940, SM8976, MSM8937, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDA 1630, SDA 1630, SDA 1630, SDA 1650, SM	oice & 9, 8, 5, 7, 5, 40, 5, 4660, M439, M632, M670, M850, 5, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	bulleti	n		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape Snape Snape Snape Snape Snape Snape Snape Snape	nation d k of addr done or s in SDI dragon C dragon C dragon I dragon W dragon W	ress rang the Sys code. in uto, ompute onnectiv onsume adustria lobile,	ge DBG , vity, er IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			Netwo APQ8 MDM <sup>1</sup> MSM8 MSM8 MSM8 QCS4 <sup>1</sup> SDA6 SDM6 SDM6 SDM6 SDM8 Snapo	lragon_H	APQ80 Q8053, SM8905 SM8917, SM8937, SM8953, cobar, Q 05, QM2 845, SDM 450, SD 710, SD	CS404, 215, 4429, M630, M660, M845,				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear: APQ8 APQ8 MDM' MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8	P modul out side it receiv essage. is Snapdra dragon Ir dragon, MI 9615, MI 9635M, I 9635M, I 9639, MS 3909W, I 8909W, I 890W, I	e may active malforms	ccess idary ormed dragon inpute, r IOT, dragon oice &  9,  8,  40,  7,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/587
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	l	Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			QM21 SDA8- SDM6 SDM7 SDX2- SM61 SM82 Snapo	ar, QCM: 5, SC818 45, SDM 50, SDM 10, SDM 0, SDX24 50, SM7: 50, lragon_H 130, SXI D: CVE-	30X, SDA 429, SDI 630, SD 660, SD 845, SD 7, SDX55 150, SM High_Me R2130	A660, M439, M632, M670, M850, , 8150,				
N/A	21-11-2019	7.2	copy for the Paramare from the	e invoking from fd of secure had been noned for a some noned fragon Coloragon Working in the secure of the secure for a some for a some noned fragon Working in the secure for a some noned fragon Working in the secure for a some noned for a some	or local bouffer, eing popsecure in Snape gon Coronsume adustria lobile, oice & Maried and APQ80 (28053, 28096A) (28096A) (28096A	ouffer oulated dragon npute, vity, r IOT, l IOT, U, 09, U, 5, 0, 98, 215, M429, M630,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/588
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM8 SM81 Snapo , SXR2	70, SDM 850, SM6 50, dragon_F 1130, SX <b>D : CVE-</b>	150, SM Iigh_Me R2130	7150, d_2016				
Out-of- bounds Read	21-11-2019	2.1	Trust memore result Snapo Snap	dragon Variation Maragon Variagon Varia	do an ariwhich we S in auto, onnectivonsume adustria fobile, foice & More and a APQ80 (28096, IPQ8074), SM8940, SM8940, GM8940, GM8940	bitrary vill vity, r IOT, l IOT, lusic, 17, 4, 4, 1439, d_2016	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/589
msm8940_fir	mware		While processing Attach							
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi result in Sna Snapo Snapo Snapo Snapo	e process t messag tion is no cing into apdragon dragon C dragon I dragon I dragon I dragon I e, Snapd	e, Valid ot met an infin Auto, ompute onsumendustria	exit ite loop , r IOT, l IOT, dragon	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MSM8- 031219	/590
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SDM4 SDM6 SDM6 SDM6 SDM6 SDM8 SDX58 SM81 Snapo	c, Snapdr ables in 2 017, APC 096AU, 2 9150, MI 9615, MI 9635M, I 9635M, S 8905, MS 8905, MS 8909W, I 8920, MS 8976, MS 8976, MS 8976, MS 8976, MS 8976, SDM 60, SDM 645, SDM 645, SDM 65, SM61! 50, SM8 dragon_H 1130, SX D: CVE-	APQ800 Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 SM8909, MSM891 SM8953, SM895	8, 5, 7, 6, 40, 5, 40, 5, AU, M215, A845, M450, M636, M710, X20, 150,				
Use After Free	21-11-2019	2.1	daem static freed in Sna Snapo Snapo Snapo Snapo Mobil Music Wears	on shute object in from a napdragon Calragon Calragon Calragon Indicates In a supplies in Application In a supplies in Application In Indication Indica	down dunstance grant properties on sume andustria parties on Vagon Vagon Q8053,	e to getting places  vity, or IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909, MSM8909, MSM8909, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM896AU, MSM8998, Nicobar, QCS605, SDA660, SDA455, SDM450, SDM660, SDM845, SDM20, SDM24, SM6150, SM7150, SM8150, SM8250, SXR2130	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index  21-11-2019  Array Index  21-17-2019  Array Index  Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8099, APQ8017, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  Out-of-bounds access can occur in camera driver due to improper due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Mobile, Mttps://ww w.qualcom pany/produ ct- security/bu lletins/octo ber-2019- bulletin				MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150,		
to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8098, MDM9206, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8905, MSM8909, MSM8905, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8933, MSM8996AU, MSM8933, MSM8996AU, MSM8933, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20						
CVE 15 . CVE 2017 10303	Validation of	21-11-2019	4.6	occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM896AU, MSM8988, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660,	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-	MSM8-

(CVSS)

Weakness	Publish Date	CVSS	ı	Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
Out-of- bounds Read	21-11-2019	10	while session messar un-interest of the session messar un-interest of snaped Snaped Snaped Snaped Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM8 SDM8	r over reparsing on manages if new dragon Adragon College on the ground of the ground	downlingement of tworks alues in uto, ompute onsume industria of, Snap ragon Vagon APQ800 Q8053, APQ809 DM9625 DM9625 DM9625 DM9655 DM8976, SD855 DM568, SD855 DM568, SD855 DM568, SD855 DM568, SD855 DM568 DM968 DM9	nk OTA sends  , er IOT, d IOT, dragon oice &  9, 8, 5, 40, 5, 17, , 18, 298, CS605, A660, M439, M632, M632, M632, M632, M630, M632, M630, M630, M630, M630, M630, M630, M631, M630, M631,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/593
Improper Authenticati	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can				https://ww w.qualcom m.com/com		O-QUA- MSM8-	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	CID
on			result	into aut	henticat	tion	pany/	produ	031219	/594
			bypas	s of NAS	in		ct-			
			Snapo	lragon A	uto,		securi	ty/bu		
			Snapo	lragon C	ompute	,	lletins	octo/		
			Snapo	lragon C	onsume	r IOT,	ber-20	19-		
			Snapo	lragon Ir	ıdustria	l IOT,	bulleti	n		
			^	lragon Io	•	O				
				e, Snapd	_	oice &				
				, Snapdr	•					
				ables in A	•	9,				
			_	017, APC	•	_				
			_	096AU, A	•					
				9150, MI		•				
				9206, MI		•				
				9615, MI						
				9635M, I		•				
				9650, MI						
				3905, MS						
				3909W, N		•				
				3920, MS	•					
				3939, MS	•					
				3953, MS	•					
				3996AU,		•				
				ar, QCM						
			_	.5, SC818		•				
				45, SDM	,	,				
				50, SDM 36, SDM	•	•				
				30, SDM 10, SDM	•	,				
				10, SDM 0, SDX24	•	•				
				•	•	•				
			SM82	50, SM7	150, SM	0130,				
				ou, lragon_H	ligh Mo	d 2016				
			^	130, SXI	•	u_2010				
			·	•						
				D : CVE-						
Improper				nation d			https:/	•		
Restriction				k of addr			w.qual		O-QUA-	
of	21-11-2019	2.1		done on	•		m.com/com		MSM8-	
Operations				s in SDI			pany/produ		031219	/595
within the			Snapo			ct-				
Bounds of a			Snapdragon Compute,					ty/bu		
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Memory Buffer			Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 MDM9 MSM8 MSM8 MSM8 QCS40 SDA6 SDM6 SDM6 SDM6 SDM6 SDM8 Snapo	dragon_F	onsume ndustria Mobile, Yoice & M Vired e and n APQ80 Q8053, SM8905 SM8937, SM8937, SM8953, cobar, Q M205, QM2 1450, SD M450, SD M450, SD M450, SD M450, SD M450, SD M450, SD	r IOT, l IOT, lusic, 09, , CS404, 215, M429, M630, M660, M845,	lletins, ber-20 bulleti	19-		
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Weara APQ8 APQ8 MDM MDM MDM MDM MDM	P modulout side it receives sage. Snapdra dragon Indragon	its bour res malfo in Snapo agon Cor consume ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9605 DM9605 MDM9625	ndary ormed dragon npute, r IOT, dragon oice &  9, 8, 7, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	/com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/596
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	tch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	3905, MS 3909W, N 3920, MS 3939, MS 3953, MS 3996AU, 536, SDM 45, SDM 45, SDM 536, SDM 536, SDM 50, SDX24 50, SM7 50,	MSM8917, SM8940, SM8976, MSM89 2150, Qu 80X, SDA 429, SDI 6630, SD 6660, SD 845, SD 150, SM	98, CS605, A660, M439, M632, M670, M850,				
			CVE I	D : CVE-	2019-2	303				
N/A	21-11-2019	7.2	copy to the Param are from environment of Snapo	e invokin from fd of e secure land neters be om non so onment. Snapdra dragon C dragon I dragon W dragon W drag	or local lands ouffer, eing pope secure in Snape gon Coronsume dustria lobile, foice & March 1 APQ80 Q8053, Q8096A M9150, DM9650 GM8909, GM8920, GM892	ouffer oulated dragon mpute, vity, or IOT, l IOT, dusic, U,	https:/ w.qual m.com pany/i ct- securif lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- MSM8- 031219	/597
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	Pat	ch	NCIIP	C ID	
			MSM8 QCS46 SDA6 SDM6 SDM6 SDM8 SM81 Snapo	3953, MS 3996AU, 04, QCS6 60, SDA8 39, SDM 32, SDM 570, SM6 50, SM6 50, dragon_F 1130, SX <b>D: CVE-</b>	MSM89 605, QM2 845, SDM 4450, SD 6636, SD 1710, SD 150, SM High_Me R2130	98, 215, 4429, M630, M660, M845, 7150,				
Out-of- bounds Read	21-11-2019	2.1	Trusti memo result Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 APQ8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 Snapo	decure Kory read into DO dragon Adragon Codragon Waragon Warag	do an ar which w S in uto, onnective onsume ndustriated foice & M Vired and APQ80 28096, (PQ8074 SM8940, SM8940, GM8940, GM8940, GM8940, GM8940, GM8940, GM8940, GM8940, GM8940,	bitrary vill vity, r IOT, l IOT, fusic, 17, 4, 1439, d_2016	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MSM8- 031219	/598
msm8996_fir	mware									
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places				-		0-QUA- MSM8- 031219	/599
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Wearables in APQ8009, APQ8017, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8933, MSM8996, MSM8996AU, MSM8937, MSM8933, MSM8996, MSM8996AU, MSM8917, MSM8920, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8917, MSM8920, MSM8917, MSM8920, MSM8917, MSM8920, MSM8917, MSM8920, MSM890, MSM8996AU, MSM8917, MSM8933, MSM8996, MSM8996AU, MSM8917, MSM8933, MSM8906, MSM8996AU, MSM8917, MSM8933, MSM8996, MSM8996AU, MSM8917, MSM8933, MSM8996, MSM8996AU, MSM8917, MSM8933, MSM8996, MSM8996AU, MSM8917, MSM8933, MSM8996, MSM8996AU, MSM8917, MSM8996AU, MSM8998, Nicobar, QC\$605, SDA660, SDA645, SDM450, SDM660, SDM670, SDM710, SDM645, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130  CVE ID: CVE-2019-10490  While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Materialitais is AD09000	Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and    Copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon m.com/com pany/produ ct-security/bu lletins/octo ber-2019-bulletin				Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musio Wears APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SM61 SM82	dragon C dragon C dragon I dragon I dragon I dragon I e, Snapdr sbles in 1 017, APO 096AU, 1 9207C, M 9207C, M 9207C, M 9397, MS 3940, MS 3940, MS 3940, MS 3940, MS 3940, MS 3940, SDM 445, SDM 50, SM7 50, SM7	compute, connective consume ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9206 MDM960 SM8905 SM8905 SM8939, SM8939, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953,	vity, or IOT, I IOT, odragon foice & 9, 8, 5, 07, W, W, CS605, M450, M710, 24, 8150,	securit lletins ber-20	/octo )19-		
Networking in APQ8009,	N/A	21-11-2019	7.2	copy for the the Param are from	from fd of secure landers be om non a comment. Snapdra dragon C dragon I dragon V dragon V dragon V	or local buffer, eing popsecure in Snaperson Corsume industria Mobile, Voice & Movined e and	ouffer oulated dragon mpute, vity, or IOT, l IOT,	w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	MSM8-	/600
CV Scoring Scale (CVSS)         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10	_	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 APQ8 MDM' MDM' MSM8 MSM8 MSM8 MSM8 QCS4 SDA6 SDM6 SDM6 SDM6 SDM8 SM81 Snapo	dragon_H 1130, SX	Q8096A M9150, DM9206 DM9650 SM8909, SM8920, SM8940, SM8996, MSM89 605, QM2 8450, SDM 450, SDM 150, SM	5, 0, 98, 215, M429, M630, M660, M845, 7150,				
Out-of- bounds Read	21-11-2019	2.1	Non S Trust memo result Snapo	D: CVE- Secure Keezone to cory read a into DO dragon A dragon Codragon Waragon	ernel can do an ar which v S in uto, onnection onsume dustria lobile, foice & M Vired and a APQ80 Q8096, IPQ8074 GM8920, GM8920, GM8940, QCA808	n cause bitrary vill vity, er IOT, l IOT, Music, 17,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA- MSM8- 031219	/601
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016		
			CVE ID : CVE-2019-2318		
sdm450_firm	ware				1
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4- 031219/602

Weakness	Publish Date	cvss	ſ	Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
Use After Free	21-11-2019	2.1	daeme static freed in Sna Snape Snape Snape Snape Snape Snape Snape Mobil Music Weara APQ8 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDA66 SDM6 SDM6 SM61 SM82	etter free on shutch object in from a mandragon Chragon Chragon Indragon In	lown duastance graden Auto, ompute onnectivonsume of T, Snap ragon APQ800 Q8053, APQ809 Q805 Q805 Q805 Q805 Q805 Q805 Q805 Q805	e to getting places , vity, er IOT, l IOT, dragon oice & 9, 8, 5, 77, , W, CS605, M450, M710, 24, 8150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Improper Validation of Array Index	21-11-2019	4.6	occur to imp array Auto, Electr Snapo Snapo Snapo Snapo	f-bounds in came proper v index in Snapdra ronics Co dragon I dragon M dragon V dragon V	ra drive alidation Snapdr gon Cor onnectiv onsume ndustria Iobile,	r due n of agon nsumer ity, er IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 APQ8 MDM' MDM' MSM8 MSM8 MSM8 MSM8 CON7 SDM6 SDX20	009, APC 053, APC 098, MD 9207C, M 9640, MS 3905, MS 3909W, MS 3940, MS 3996AU, 605, SDM 0	Q8096A M9206, MDM9650 DM9650 MSM891, MSM8937, SM8953, MSM89 A660, SI	98, 0M450, M660,				
Out-of- bounds Read	21-11-2019	10	while session messar un-information of Snapor Snapor Snapor Snapor Snapor Snapor Snapor Snapor Snapor Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8 MSM8	r over reparsing on manages if netended version Adragon Adragon Indragon In	downlingement (etwork stalues in uto, ompute, onsume ndustria oT, Snap ragon Vagon APQ800 Q8053, APQ809 DM9607 DM9605 DM8900 DM9605 DM9605 DM8900 DM9605 DM8900 DM9605 DM8900 DM9605 DM8900 DM9605 DM8900 DM8	nk OTA Sends  r IOT, l IOT, dragon oice &  9,  8,  7,  40,  5,  47,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-3	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
			SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	.5, SC81; 45, SDM .50, SDM .36, SDM .10, SDX24 50, SM7 50, dragon_H .130, SX <b>D: CVE-</b>	429, SD 1630, SD 1660, SD 1845, SD 1, SDX55 150, SM High_Me R2130	M439, M632, M670, M850, 8150, d_2016				
Improper Authenticati on	21-11-2019	10	Lack of allow NAS in result bypas Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	of integral of integral of integral of into autorises of NAS dragon of integral of integra	ity check M to access which a chentical in auto, compute consume adustrial oT, Snap largon V ragon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9625 MDM9625 MDM9625 MSM8937, SM8940, MSM8937, SM8940, MSM8937, MSM8940,	k ept any can tion  or IOT, ol IOT, odragon voice & ept any can tion  8, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10	https:/w.qualm.company/jct-securitiletinsber-20bulleti	com /com produ ty/bu /octo	O-QUA-3 031219	
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publ	ish Date	CVSS		Description	on & CVE	ID	Pat	:ch	NCIIP	C ID
				SDM7 SDX2 SM61 SM82 Snapo , SXR2	lragon_I I 130, SX <b>D : CVE-</b>	1845, SD 4, SDX55 150, SM High_Me R2130 <b>2019-2</b>	M850, , 8150, d_2016 <b>289</b>				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-1	1-2019	2.1	to lack check buffer Snape	dragon_F	ress range the System the System to the Syst	ge sDBG , vity, r IOT, l IOT, Music, 09, , , CS404, 215, M429, M630, M642, M645, d_2016	https:/w.qualm.company/jct-securitiletinsber-20bulleti	lcom l/com produ ty/bu /octo	O-QUA- 031219	
Out-of- bounds Read	21-1	1-2019	7.5	SNDC array	P modul out side	e may a	ccess ndary	w.qualcom		0-QUA-	
CV Scoring Scale (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			XID m Auto, Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	nessage. Snapdradragon Colaragon Indragon Indrag	in Snapo agon Con- onsume adustria oT, Snapo ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9605 MSM8909, MSM8916, M	Iragon npute, r IOT, I IOT, dragon oice &  9,  8,  7,  40,  7,  7,  98, CS605, A660, M439, M670, M850, , 8150, d_2016	pany/j ct- securit lletins, ber-20 bulleti	produ ty/bu /octo 119-		
N/A	21-11-2019	7.2	While copy to the Param are freenviro Auto,	D: CVE- e invoking from fd of e secure le eneters be om non se onment. Snapdra dragon C	g the AP or local to ouffer, eing pop secure in Snapo igon Con	I to ouffer ulated dragon npute,	https://w.qualm.com pany/jct- securit lletins/ber-20	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo Snapo Infras Netwo APQ8 APQ8 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SDM8 SM81 Snapo	dragon Colragon Maragon Waragon Waragon Waragon Waragon Waragon Waragon Waragon, APC 096, APC 098, MD 9205, MD 9607, SD MB 9607, SD	ndustria Mobile, Moice & M Vired and APQ80 Q8053, Q8096A M9150, DM9206 DM9650 SM8920, SM8940, SM8940, SM8940, SM8940, SM896, MSM89 MSM896, MSM	1 IOT,  Music,  109,  U,  105,  109,	bulleti	n		
Out-of- bounds Read	21-11-2019	2.1	Trustomemo result Snapo	ecure Kezone to o ory read into DO dragon C dragon I dragon V dragon V dragon V dragon V etructure orking ir 053, APO	do an ar which was in auto, connective consume andustria Mobile, Moice & M Vired and and APQ80	bitrary vill vity, er IOT, l IOT, Music,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318		
sm8250_firm	ware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SM82- 031219/611

Weakness	Pu	blish Date	cvss		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
				SDX5 SM81 Snapo	345, SDM 5, SM61 50, SM8 dragon_I 1130, SX	50, SM7 250, High_Me	150,				
				CVE I	D : CVE-	2019-2	335				
Use After Free	21-	-11-2019	2.1	daem static freed in Sna Snape Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61 SM82	fter free on shute object in from a rapdragon of dragon	down dunstance nultiple n Auto, Compute Connecti Consume ndustria oT, Snap dragon Vagon APQ800 APQ809 APQ80	te to getting places  , vity, er IOT, edragon voice & 19, 107, 107, 107, 107, 107, 107, 107, 107	https:/w.qualm.com pany/ct- securi lletins ber-20 bulleti	ty/bu /octo	0-QUA- 031219	
Buffer Copy without Checking Size of Input	21	-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater				https:/ w.qual m.com pany/	com com	0-QUA- 031219	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
('Classic Buffer Overflow')			Snapo Snapo Snapo Snapo Snapo Snapo Snapo APQ8 MDM MDM MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	max rate dragon A dragon C dragon C dragon In dragon I dragon V 017, APC 096AU, I 9207C, M 9650, MS 377, QCA 605, QCS 45, SDM 645, SDM 50, SMS 50, SMS	ompute onsume onnectivonsume onsume o	cr city, er IOT, d IOT, dusic in 06, 07, c, AU, CS605, M710, 150, R2130	ct- securii lletins ber-20 bulleti	/octo )19-		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from a source that the potent buffer Snape	tmap file any un-a e, there i he bitma tially cau dragon A dragon C dragon C dragon C dragon C dragon M dragon W 016, APC 098, MD 3996AU, ar, QCS4	is a possip can use stack w. in uto, ompute onnectivonsume onsume onsume foice & March 1980 March 1	cated sibility k  k  vity, er ity, er IOT, al IOT, U,  198, 6605,	https:/ w.qual m.com pany/j ct- securif lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDM8 SM61 SM82	45, SDM 660, SDM 845, SDM 50, SM7 50, SXR2 <b>D : CVE-</b>	670, SD 850, SD 150, SM 130, SX	M710, X24, 8150, R2130				
Out-of- bounds Read	21-11-2019	10	Buffer while session messar un-information Snaper S	r over reparsing on manages if netended with the design of	ad can hadownling gement of tworks shalues in uto, ompute onsume adustria of, Snap ragon vagon APQ800 Q8053, APQ809 DM9625 DM9625 DM9655 DM8976, SD855 DM560, SD855 DM560, SD855 DM560, SD855 DM555 DM5	nappen nk OTA sends or IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 47, 48, 68, 68, 68, 68, 68, 68, 68, 68, 68, 6	https:/w.qualm.company/jct-securitelletins/ber-20	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8996, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM82- 031219/616

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			CVE I	D : CVE-	2019-2	289				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modulout side it receive it receive iessage. Snapdradragon Idragon Idragon, M. 19635	its bounces malforing Snapon Consumer and Stragon Veragon APQ800 DM9605 DM9605 DM9605 DM9655 SM8909 MSM8937 SM8940 BMSM8937 SM8940 BMSM8937 SM8940 BMSM895 SM895 S	ndary ormed dragon mpute, er IOT, al IOT, odragon Voice & 19, 16, 17, 17, 17, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9	
sxr2130_firm	ware						1			
Loop with Unreachable	21-11-2019	5		process t messag	•		https:/ w.qual	-	0-QUA-9	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[	Descriptio	n & CVE	ID	Pat	ch	NCIII	PC ID
Exit				tion is no			m.com	•		
Condition				ing into		ite loop	pany/	produ		
('Infinite				pdragor	•		ct-			
Loop')			-	lragon C	•		securi			
			-	lragon C			lletins			
			•	lragon Ir			ber-20			
			•	lragon Id	•	O	bulleti	n		
				e, Snapd	_	oice &				
				, Snapdr	•	_				
				ables in A	•	9,				
			_	017, AP(	•					
			_	096AU, <i>I</i>	•					
				9150, MI		•				
				9206, MI		•				
				9615, MI		•				
				9635M, I		•				
				9650, MI						
				3905, MS						
				8909W, N		•				
				3920, MS	•					
				3940, MS	•					
				3976, MS		AU,				
				3998, Nic 150, QC		M21E				
			-	30X, SDA	_					
				29, SDM	•	•				
				30, SDM	•	•				
				60, SDM	•	•				
				45, SDM	•	•				
				5, SM615	•	•				
				50, SM82	•	150,				
				lragon_H		d 2016				
				.130, SXI		u_2010				
				D : CVE-						
				quent us			https:/	•		
				er may r			w.qual			
Use After	04 44 0040	4.0		ry corru	-		m.com	-	O-QUA-	-SXR2-
Free	21-11-2019	4.9			ree issue. in pany/p			produ	031219	
			_	lragon A			ct-			-
				ompute		securi				
			Snapdragon Connectivity,					/octo		
CV Scoring Scal	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6					7-8	8-9	9-10
(CVSS)				279						

Weakness	Pul	blish Date	CVSS		Description	on & CVE	Pat	:ch	NCIIP	C ID	
				Snapo Snapo Snapo Infras Netwo QCS4 SM71	dragon C dragon I dragon V dragon V dragon V etructure orking in 04, SDX5 50, SM8	ndustria Mobile, Moice & M Wired e and n MDM9 55, SM62 150, SXI	ll IOT, Music, 205, 150, R2130	ber-20 bulleti			
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-	-11-2019	7.2	lack of array image Snape Snap	f bound f check of size white e elf segre dragon A dragon O dragon I dragon I dragon V dragon V etructure orking in 04, QCS6 570, SDM 550, SDX 50, SM7 130, SXF	of whilte ile readi nents. in ompute connecti consume ndustria Mobile, Vired e and n MDM9 505, SDA 1710, SDA 1710, SDA 1710, SM 22130	elist ng the  , vity, er IOT, al IOT, M845, M845, 8150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- 031219	
Use After Free	21-	-11-2019	2.1	daem static freed in Sna Snapo Snapo Snapo Snapo Snapo	fter free on shutc object in from a r apdragon C dragon C dragon I dragon I dragon I e, Snapo	down dunstance nultiple n Auto, dompute donnecti donsume ndustria	e to getting places , vity, er IOT, al IOT, odragon	https://w.qualm.com pany/jct- securitelletins ber-20 bulleti	lcom l/com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	Pat	ch	NCIIP	C ID	
			Wear APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61 SM82	c, Snapdrables in 2017, APC 096AU, 29150, MS 9207C, MS 9909, MS 8937, MS 8996, MS 8996, MS 8996, SDA 860, SDA 860, SDA 860, SDA 50, SM7 50, SM7	APQ800 Q8053, APQ809 DM9206 MDM960 SM8905 SM8909 SM8939, SM8939, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953,	8, 5, 77, W, CS605, M450, M710, 24,				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer wlan rates elements than in Snapor Sn	r overflomodule for extendent lengt max rate dragon Caragon Caragon Caragon Maragon Ma	w can o if suppo ded rate h is great leng auto, ompute onsume onsume onsume ondustria Mobile, Toice & MQ8053, MDM92 MDM960 SM8905 Nicobar CA6574, A9379, S405, Q0	ccur in rted es ater th in rted ity, r IOT, IOT, IOT, Ausic in CS605,	https:/w.qualm.com pany/jct- securif lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6					7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			SM81	45, SDX 50, SM8	250, SXI	R2130				
				D : CVE-						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from a source that the potent buffer Snape	tmap file any un-a e, there he bitma tially ca roverflo dragon A dragon C dragon C dragon C dragon C dragon W 1016, APC 098, MD 3996AU, ar, QCS4 55P, SC8 45, SDM 45, SDM 45, SDM 50, SM7 50, SXR	is a possing can use stack w. in auto, compute connective consumendustria Mobile, Mos	cated bibility k  k  vity, r ity, r ity, l IOT, l I	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- 031219	
Out-of- bounds Read	21-11-2019	10	while session messa un-int Snapo Snapo Snapo Snapo Snapo	r over re parsing on manag ages if no tended v dragon A dragon C dragon I dragon I dragon I e, Snapd	downlingement of the setwork so walues in the setwork sompute consume and ustria to T, Snap	nk OTA eends , r IOT, l IOT, dragon	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	Pat	ch	NCIIP	CID	
			Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	c, Snapdrables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MS 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3953, MS 3953, MS 3953, MS 300, SDM 45, SDM 45, SDM 45, SDM 45, SDM 45, SDM 50, SDX24 50, SM7 50, SM7 50, SM7	APQ800 Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 GM8909 MSM8937 GM8940, SM8940, SM8940, SM8976, MSM89 2150, Q 80X, SD, 429, SD, 1630, SD, 1630, SD, 1630, SD, 1630, SD, 1630, SD, 1645, SD, 1650, SM	18, 5, 7, 5, 40, 5, 17, 198, CS605, A660, M439, M632, M670, M850, 5, 8150, d_2016				
Improper Authenticati on	21-11-2019	10	allowan NAS m result bypas Snapo Snapo Snapo Snapo Mobil Music Weara	of integrals MODEI nessages into aut is of NAS dragon A dragon C dragon I dragon I dragon I c, Snapdr ables in A	M to acc s which thentica s in outo, ompute onsume ndustria oT, Snap lragon V ragon	ept any can tion er IOT, al IOT, odragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM7 SDX2 SM61 SM82 Snapo , SXR1	096AU, A 9150, MI 9206, MI 9615, MI 9635M, II 9635M, II 8905, MS 8905, MS 8920, MS 8939, MS 8953, MS 8953, MS 8953, MS 805, SDM 15, SC818 16, SDM 10, SDM 10, SDM 10, SDM 10, SDM 1130, SM 1130, SX 1130, SX 1130, SX 1130, SX	DM9205 DM9607 DM9625 MDM9655 MSM8909, MSM8916 SM8937, SM8940, SM8976, MSM89 2150, Qu 80X, SDA 429, SDA 1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	5, 7, 6, 40, 6, 7, 27, 27, 28, 28, 28, 28, 38, 46, 48, 48, 48, 48, 50, 61, 61, 61, 61, 61, 61, 61, 61, 61, 61				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM	P modul out side it receivnessage. It sapped it agon It dragon It de Snaped it de	its bounders malfoling Snapon Coronsume andustria porto T, Snapon Varagon Varagon Varagon Q8053, APQ809 DM9205 DM9607 DM9625	ndary ormed dragon npute, r IOT, l IOT, dragon oice &  9,  8, 6, 7,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	Pat	ch	NCIIP	C ID	
			MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	9650, M. 8905, M. 8909W, I 8920, M. 8939, M. 8953, M. 896AU, 9ar, QCM 950, SC818 950, SDM 950, SDM 950, SDM 950, SM7 950, SM7 950, SM7	5M8909, MSM8915 5M8940, 5M8976, MSM89 2150, Q 80X, SD 429, SD 1660, SD 1660, SD 1845, SD 150, SM	98, 98, CS605, A660, M439, M632, M670, M850,				
			CVE I	D : CVE-	2019-2					
N/A	21-11-2019	7.2	copy to the Paramare from Environment of Snapo S	e invoking from fd of secure landers be om non a comment. Snapdra dragon Of dragon Maragon Walragon Walragon, Maragon Walragon, Maragon, M	or local louffer, eing popsecure in Snapelgon Coronsumendustria dobile, foice & Mored and APQ80 Q8053, Q8096A M9150, DM9206 GM8909	ouffer oulated dragon mpute, vity, er IOT, l IOT, Uusic, U,	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-3	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6					7-8	8-9	9-10

Weakness	Publish Date	CVSS	l	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 QCS46 SDA66 SDM6 SDM6 SDM8 SM81 Snapo	3937, MS 3953, MS 3996AU, 04, QCS6 60, SDA6 39, SDM 50, SDM 50, SM6 50, dragon_H 130, SX <b>D: CVE-</b>	5M8996, MSM89 505, QM2 845, SDM 450, SD 1636, SD 1710, SD 150, SM High_Me R2130	98, 215, M429, M630, M660, M845, 7150,				
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID: CVE-2019-2329				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
apq8016_firm	iware									
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6		6-7	7-8	8-9	9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID: CVE-2019-2251		
sa6155p_firm	ware		CVE 1D . CVE 2017 2231		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SA61- 031219/630

3-4

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			SM82	50, SM7 50, SXR	1130, SX	R2130				
			CVE I	D : CVE-	2019-2	251				
sc8180x_firm	ware		T				T			
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi result in Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	e process t messag tion is n cing into apdragon dragon of dragon of dragon In dragon I	ge, Valid ot met an infin in Auto, compute on Sume industria oT, Snap largon Vagon APQ809 DM9607 DM9607 DM9605 SM8909, MSM891 SM8953,	exit ite loop , r IOT, l IOT, dragon oice & 9, 8, 6, 7, 40, 6, 7, AU, M215, A845, M450, M636, M710, X20, 150, d_2016	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	De	escriptio	n & CVE	ID	Pat	ch	NCIIP	CID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	Snapdra Snapdra Snapdra Snapdra Snapdra APQ809 MSM89 Nicobar SA6155 SDA845 SDM66 SDM84 SM6150 SM8250	ny un-a there i e bitma ally cau overflow agon A agon Co agon Co agon Ir agon M agon W 16, APO 98, MD 96AU, r, QCS4 5, SDM 60, SDM 5, SDM 0, SM7 10, SXR1	uthentics a poss p can use stack w. in uto, ompute, onnectivonsume ndustria lobile, oice & MQ8096AMM9205, MSM8905, QCS180X, SI630, SDI670, SDI650, SDI	cated ibility k  vity, r ity, r IOT, l IOT, l IOT, Music in U, 98, 605, DA660, M636, M710, X24, 8150, R2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Out-of- bounds Read	21-11-2019	10	Buffer of while p session messag un-inte Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Music, S Wearab APQ803	arsing manages if need veragon Coagon Irragon Icragon	downlingement (stwork stalues in uto, ompute, onsume ndustria oT, Snap ragon Vagon Q8053,	nk OTA ends  r IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	9150, MI 9206, MI 9615, MI 9635M, I 9650, MS 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3953, MS 3953, MS 36, SDM 45, SC818 45, SDM 45, SDM 50, SDX24 50, SM7 50, SM7 50, SM7	DM9607 DM9625 MDM9655 SM8909, MSM891 SM8940, SM8940, SM8976, MSM89 2150, Qu 80X, SDA 429, SDI 1630, SD 1845, SD 150, SM High_Me R2130	7, 6, 40, 6, 7, 98, CS605, A660, M439, M670, M850, 5,				
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,			https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219		
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	tch	NCIIP	C ID
			MDM MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	dragon_H 1130, SXI	DM9655 M8909, MSM891 SM8937, SM8976, MSM89 2150, Q0 30X, SDA 429, SDA 660, SD 660, SD 845, SD 7, SDX55 150, SM	98, CS605, A660, M439, M632, M670, M850, ,				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MDM MSM8	D: CVE-P modulout side it receives sage. it sages it sage	e may active the may active some on the consumer of the consum	ccess indary ormed dragon inpute, r IOT, dragon foice &  9,  8, 6, 7, 40, 6, 17,	https:/ w.qual m.com pany/s ct- securit lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303		
sdm850_firm	ware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8- 031219/636

3-4

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

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, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID: CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130  CVE ID: CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	0-QUA-SDM8- 031219/637
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDM8- 031219/638
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			Electr Snapo Snapo Snapo APQ8 APQ8 MSM8 Nicob SA61! SDA8 SDM6 SDM8	dragon Conics Collingon Collingon Indragon Maragon Work, APC 098, MD 3996AU, 125, SDM 145, SDM 145, SDM 150, SM7 150, SM7 150, SM7 150, SXR1	onnectivonsume ndustria lobile, oice & M 28096A M9205, MSM89 05, QCS 180X, SD 630, SD 670, SD 850, SD	ity, r IOT, l IOT, fusic in U, 98, 605, DA660, M636, M710, X24, 8150,				
Out-of- bounds Read	21-11-2019	10	Buffer while session messar un-information Snapor Snapor Snapor Snapor Snapor Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MSM8 MSM8	r over reparsing on manages if netended veragon Caragon Caragon Indragon In	ad can had can	nappen nk OTA rends r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5,	https:/ w.qual m.com pany/ct- securif lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 Nicob QM21 SDA8- SDM4 SDM7 SDX20 SM61 SM82 Snapo , SXR1	3953, MS 3996AU, ar, QCM 5, SC818 45, SDM 50, SDM 10, SDM 0, SDX24 50, SM7 50, dragon_H 130, SX	MSM89 2150, Qu 30X, SDA 429, SDI 630, SD 6660, SD 845, SD 5, SDX55 150, SM High_Me R2130	98, CS605, A660, M439, M632, M670, M850, ,				
Improper Authenticati on	21-11-2019	10	allowing NAS in result bypas Snapo Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integrals MODEI nessages into autors of NAS dragon A dragon C dragon In d	M to accombined to accombine the computer of t	ept any can tion r IOT, l IOT, dragon coice & 9, 8, 7, 7, 40, 15, 17, 17, 17, 18, 198, 198, 198, 198, 198, 198, 198,	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9	
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

QM215, SC8180X, SDA660, SDA845, SDM429, SDM430, SDM430, SDM430, SDM632, SDM450, SDM630, SDM632, SDM50, SDM50, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SM8250, SM8250, SM82130   CVE ID : CVE-2019-2289	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8990, MSM8917, MSM8920, MSM8937, MSM8990, MSM8938, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA660, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130				SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130		
	Restriction of Operations within the Bounds of a Memory	21-11-2019	2.1	to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-	_

(CVSS)

Weakness	Publish Date	cvss	[	Descriptio	n & CVE	ID	Pat	ch	NCIII	PC ID
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapd Snapd Snapd Mobil Music Weara APQ80 MDM9 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM7 SDX20 SM61 SM82 Snapd , SXR1	P modul out side it receiv lessage. i Snapdra lragon Ir lragon, MI lragon, MI lragon, MS lragon, MS lragon, SNI lragon, SNI lragon, SXI lragon,	its bour es malforin Snapor Corronsume industria oT, Snapor RAPQ800 Q8053, APQ809 DM9625 DM9625 DM9655 GM8909, MSM891 GM8937, GM8940, GM8976, MSM8976, MSM8976, GMSM8976, GMSM89	ndary ormed dragon inpute, or IOT, I IOT, I IOT, I IOT, I IOT of	https:/w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com orodu cy/bu /octo 19-	O-QUA- 031219	
N/A	21-11-2019	7.2	copy f to the Paran	invokin from fd c secure l neters be	or local bouffer, eing pop	ouffer	https://w.qual m.com pany/j	com /com	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID					ch	NCIIP	CID
			Auto, Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 APQ8 APQ8 MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SM81 Snapo	onment. Snapdra dragon O dragon I dragon V dragon, M dragon, M dragon, M dragon, M dragon, M dragon, SD dragon, SD dragon, SD dragon, SX D: CVE-	agon Cor Connective Consume Industria Mobile, Voice & M Vired e and n APQ80 Q8053, Q8096A DM9150, DM9206 DM9650 SM8940, SM8996, MSM86, MSM896, MSM806, MSM896, MSM86,	npute, vity, er IOT, l	securit lletins, ber-20 bulleti	octo 19-		
mdm915_firn	nware									
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon				https:/ w.qual m.com pany/p ct- securit lletins, ber-20 bulleti	com /com orodu cy/bu /octo 19-	O-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Mobil Music Wears APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SC818 SDM4 SDM6 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	e, Snapdr ables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 9650, MS 3905, MS 3905, MS 3905, MS 3976, MS 3976, MS 3976, MS 3976, MS 3976, SDM 60, SDM 60, SDM 50, SM615 50, SM615 1130, SXI	Tragon V Tragon V Tragon V APQ800 Q8053, APQ809 DM9607 DM9605 DM9655 MB9655 SM8937, SM8937, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM896, SOBAR, SD 1632, SD 1632, SD 1630, SM7 250, High_Me R2130	Toice &  9,  8,  6,  7,  6,  40,  6,  17,  AU,  M215,  A845,  M450,  M636,  M710,  X20,  150,  d_2016				
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/645
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	Pat	ch	NCIIP	CID	
			MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> SDM <sup>o</sup> SDA <sup>o</sup> SDM <sup>o</sup> SD	lragon_F I 130, SX	DM9205 DM9607 DM9625 MDM9645 SM8909, MSM891 SM8937, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDA 1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	98, CS605, A660, M439, M632, M670, M850, ,				
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2289		
qcm2150_firm	nware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCM2- 031219/647

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	on & CVE	Pat	ch	NCIIP	C ID	
			MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9650, MI 3905, MS 3909W, NS 3920, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDM 30X, SDM 30, SDM 345, SDM 345, SDM 345, SM615 30, SM82	5M8909, MSM8915, SM8953, SM8996, cobar, S605, Ql 439, SD 6632, SD 6632, SD 6670, SD 6850, SD 50, SM72	AU, M215, A845, M450, M636, M710, X20,				
			CVE I	D : CVE-	2019-2	335				
Out-of- bounds Read	21-11-2019	10	while session messar un-introduced Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MDM MDM MDM MDM MSM8 MSM8	r over reparsing manages if netended valuagen Caragon Caragon Internation Inte	downlingement (etwork stalues in uto, ompute onsume ndustria oT, Snapuragon Vagon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9655 MB969, MSM891	nk OTA Sends  r IOT, I IOT, dragon Soice &  9,  8, 5, 7, 40, 6,	https:/ w.qual m.com pany/j ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	[	Descriptio	n & CVE	ID	Pat	:ch	NCIIP	C ID
			MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX20 SM61 SM82 Snapo	3939, MS 3953, MS 3996AU, ar, QCM2 5, SC818 45, SDM 36, SDM 10, SDM 10, SDX24 50, SM72 50, lragon_H	5M8976, MSM89 2150, Q0 80X, SDA 429, SDI 6630, SD 6660, SD 845, SD 150, SM8	98, CS605, A660, M439, M632, M670, M850, 5, 8150,				
Improper Authenticati on	21-11-2019	10	Lack of allows NAS in result bypas Snapod Snapod Snapod Snapod Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MS	of integrics MODEM nessages into autorises of NAS dragon Adragon Coloragon Iragon Iragon, MI 19635M, MI	ity check M to accombined to chenticate in auto, ompute, onsume adustria oT, Snap ragon APQ800 Q8053, APQ809 DM9205 DM9625 DM9625 MDM9625 MDM9625 MDM9625 MSM8909, MSM8916, SM8940, SM8940,	ept any can tion  r IOT, dragon oice &  9, 8, 5, 40, 5,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA-0 031219	-
			1,191,10	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	1.1014107	, O,				

Weakness	Publish Date	CVSS	·					ch	NCIIP	C ID
			QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	ar, QCM; 5, SC818 45, SDM; 50, SDM; 10, SDM; 0, SDX24 50, SM7; 50, dragon_H; 1130, SXI	30X, SDA 429, SDI 630, SD 660, SD 845, SD 7, SDX55 150, SM High_Me R2130	A660, M439, M632, M670, M850, , 8150,				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	P modulout side it receives age. is Snapdra dragon Ir dragon, MI 9615, MI 9635M, Ir dragon, MS 39053, MS 3939, MS 3953,	its bour es malfo in Snapo gon Cor onsume idustria oT, Snap ragon V agon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9645 SM8909, MSM891 SM8937, SM8940, SM8940, SM8976, MSM89 2150, Q0 BOX, SDA 429, SDA	ndary ormed dragon inpute, r IOT, dragon oice & 9, 8, 5, 7, 7, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,	https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID: CVE-2019-2303		
sdx55_firmwa	are				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX5- 031219/651

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130		
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID: CVE-2019-2336	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDX5- 031219/652
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDX5- 031219/653

	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2339		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM630, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX5- 031219/654
Improper	21-11-2019	10	Lack of integrity check	https://ww	O-QUA-SDX5-
	<u> </u>			l	l

Weakness	Publish Date	cvss	I	Descriptio	n & CVE	Pat	ch	NCIII	PC ID	
Authenticati			allow	s MODEN	I to acc	ept any	w.qual	com	031219	655
on			NAS n	nessages	which	can	m.com	/com		
			result	into aut	hentica	tion	pany/p	orodu		
			~ ~	s of NAS			ct-			
			_	lragon A			securit			
				lragon C			lletins			
			*	lragon C		•	ber-20			
			_	lragon Ir			bulleti	n		
			^	lragon Io	•	•				
				e, Snapd	•	oice &				
				, Snapdr	_	0				
				ables in A	-	9,				
			·	017, AP(	•	O				
			~	096AU, <i>I</i> 9150, MI	•	•				
				9130, MI 9206, MI						
				9615, MI						
				9635M, I						
				9650, MI						
				3905, MS		•				
				3909W, N	•					
				3920, MS		•				
				3939, MS						
				3953, MS						
				3996AU,						
			Nicob	ar, QCM	2150, Q	CS605,				
			QM21	5, SC818	30X, SD <i>A</i>	A660,				
			SDA8	45, SDM	429, SDI	M439,				
			SDM4	50, SDM	630, SD	M632,				
			SDM6	36, SDM	660, SD	M670,				
			SDM7	10, SDM	845, SD	M850,				
			SDX2	), SDX24	, SDX55	,				
			SM61	50, SM7	150, SM	8150,				
			SM82	-						
				lragon_H		d_2016				
			, SXR1	130, SX	R2130					
			CVE I	D : CVE-	2019-2	289				
			SNDC	P modul	e may a	ccess	https://ww			
Out-of-	21-11-2019	7.5	array out side its boundary					com	O-QUA-	
bounds Read	21 11 201 <i>)</i>	7.0	when it receives malformed					/com	031219	9/656
			XID message. in Snapdragon					orodu		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapd Snapd Snapd Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA84 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapd	Snapdra dragon Indragon Indrag	onsume adustria of, Snap ragon Vagon APQ800 DM9605 DM9605 DM9605 DM9655 DM9655 DM9655 DM9655 DM9655 DM9655 DM9655 DM9655 DM9655 DM8976, SM8976, SM8976, SM8976, SM8976, SD855 DM50, SD8660, SD86600, SD866000, SD86600, SD86600, SD86600, SD86600, SD86600, SD86600, SD866000, SD86600, SD866000, SD8660000, SD8660000, SD8660000, SD8660000, SD86600000000000000000000000000000000000	r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, M439, M632, M670, M850, , 8150,	ct- securit lletins, ber-20 bulleti	octo 19-		
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired				https://w.qual m.com pany/j ct- securit lletins/ ber-20	/com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
			Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130				bulleti	n		
			CVE I	D : CVE-	2019-2	329				
apq8064_firm	iware						T			
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user stand user stand user stand user stand stand stands and stan	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297				//ww com /com orodu ty/bu /octo 19- n	O-QUA- 031219	•
apq8096_firm	iware									
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer,				https:/ w.qual m.com	com	0-QUA- 031219	_
CV Scoring Scal	e 0-1	1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	ch	NCIII	PC ID
weakness	Publish Date	CVSS	Paramare from environ Auto, Sanapad Sa	neters become non somment. Snapdradragon Calragon Iragon Iragon Williagon Wi	eing pope secure in Snape igon Cor onnectivonsume industria Mobile, foice & Movined and APQ80 (28053, Q8096A (28096A) (2	oulated dragon inpute, vity, r IOT, l	pany/j ct- securit lletins ber-20 bulleti	produ ty/bu /octo 119-	NCIII	CID
Out-of- bounds Read	21-11-2019	2.1	Trustz memo result Snapd Snapd Snapd Snapd	ecure Ke zone to d ory read into DO lragon A lragon C lragon Ir lragon M	do an ar which w S in uto, onnectiv onsume ndustria	bitrary vill vity, r IOT,	https://w.qualm.com pany/jct- securit lletins/ ber-20	com /com produ ty/bu /octo	0-QUA- 031219	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016	bulletin	
sda660_firmv	varo		CVE ID : CVE-2019-2318		
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6- 031219/661

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, 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, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-SDA6- 031219/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8937, MSM8933, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA645, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130  CVE ID: CVE-2019-10490	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-SDA6- 031219/663
				, , ,	
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-SDA6- 031219/664
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Pu	blish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
				Snapo APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8	Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20						
				CVE I	D : CVE-	2019-1	0503				
Out-of- bounds Read	21-	-11-2019	4.6	in fast to impose while from Snapos Snapos Snapos Snapos APQ8 MSM8 QCN7 SDA6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8996AU, MSM8996AU, MSM8996AU, SDX20, SDX24				//ww lcom produ ty/bu /octo )19- n	0-QUA- 031219	
Buffer Copy without Checking Size of Input ('Classic Buffer	21-	-11-2019	7.2	from source that the potential	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in				//ww com /com produ	0-QUA- 031219	
CV Scoring Scal (CVSS)	е	0-1	1-2	2-3	3-4 4-5 5-6			6-7	7-8	8-9 9-1	

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
Overflow')			Snapo Snapo Snapo Snapo Snapo Snapo Snapo APQ8 MSM8 Nicob SA618 SDM6 SDM6 SDM6 SM61 SM82	dragon Adragon Colragon Colragon Colragon Colragon Indragon Maragon Vollagon SDM Sol, SDM Sol, SDM Sol, SDM Sol, SM7 Sol, SXR1 Sol	ompute onnectivonsume onsume dustria lobile, oice & M 28096A M9205, MSM89 05, QCS 180X, SI 630, SD 670, SD 850, SD	vity, or ity, or IOT,	lletins, ber-20 bulleti	19-		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636,				https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150		
			CVE ID : CVE-2019-2268		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9625, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM8953, MSM8976, MSM8953, MSM8976, SD8450, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM630, SDM670, SDM710, SDM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2271	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-SDA6- 031219/668
CV Scoring Scal	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

(CVSS)

Authenticati on 21-11-2019 10 MDM9653, M, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8937, MSM8990, MSM8937, MSM8996, MSM8998, Nicobar, QCM2150, QC\$605, QM215, \$C8180X, \$DA660, \$DA845, \$DM429, \$DM439, \$DM450, \$DM630, \$DM632, \$DM630, \$DM632, \$DM630, \$DM630, \$DM632, \$DM630, \$DM630, \$DM632, \$DM630, \$DM845, \$DM850, \$DM20, \$DX20, \$DX24, \$DX55, \$M6150, \$M7150, \$M8150, \$M8250, \$Snapdragon_High_Med_2016, \$XR1130, \$XR2130	Weakness	Publish Date	cvss	ſ	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Restriction of 21-11-2019 2.1 to lack of address range check done on the SysDBG m.com/com 031219/670	Improper Authenticati on	21-11-2019	10	allows NAS n result bypas Snape Snape Snape Snape Snape Snape Snape Mobil Music Wear APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	s MODEN nessages into aut s of NAS lragon A lragon C lragon In lra	M to acc swhich of thentical in uto, ompute onsume industrial oT, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9625 DM9625 DM9625 DM9625 DM9635 SM8909, MSM891 SM8937, SM8940, SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM8937, SM8937,	ept any can tion  for IOT, al IOT, adragon voice & 19, 17, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18	w.qual m.com pany/j ct- securit lletins ber-20	com /com orodu cy/bu /octo 19-	_	
CV Scoring Scale	Improper Restriction	21-11-2019	2.1	to lack of address range				w.qual	com	_	
$\frac{1}{2}$	of CV Scoring Scal	e 0-1	1-2	check 2-3	done on	the Sys	5-6	m.com	/com 7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
Operations within the Bounds of a Memory Buffer			buffer Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 MDM' MSM8 MSM8 MSM8 QCS40 SDM4 SDM6 SDM6 SDM6 SDM8 Snapo	rs in SDI dragon A dragon C dragon C dragon I dragon I dragon W dragon W dragon W dragon W dragon W dragon W dragon MS 3920, MS 3	code. in uto, ompute, onnectivonsume ndustria lobile, oice & March 1980, SM8905, SM8905, SM8917, SM8953, cobar, Q 1965, SM8953, cobar, Q 1965, SM8953,	, vity, r IOT, l IOT, fusic, 09, , CS404, 215, M429, M630, M660, M845, d_2016	pany/j ct- securit lletins ber-20 bulleti	produ ty/bu /octo 119-		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing non- standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU,				https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			MDM <sup>4</sup> MDM <sup>4</sup> MSM8 QCA6 QCA9 QCS4 <sup>4</sup> SDA8 SDM8 SM81	19, IPQ8 9206, MI 9607, MI 9650, MS 3996AU, 574AU, ( 379, QCS 05, QCS 45, SDM 45, SDX 50 <b>D: CVE</b> -	DM9207 DM9640 GM8905 QCA617 QCA937 N7605, 05, SDA 636, SDA	7C, , , 74A, 77, .660, M660, 24,				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	P modul out side it receiv lessage. It sagen for a lagon for a lag	its bour es malfo in Snapo gon Cor onsume idustria oT, Snap ragon V agon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9645 SM8909, MSM891 SM8937, SM8940, SM8940, SM8976, MSM89 2150, Q0 BOX, SDA 429, SDA	ndary ormed dragon npute, r IOT, dragon oice &  9,  8,  6,  7,  40,  6,  47,  48,  CS605, A660, M439, M632,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID: CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096, APQ8096, APQ8096, MDM9205, MDM9206, MDM9205, MDM9206, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, APQ8096AU, APQ8098, MDM9650, MSM8937, MSM8940, MSM8953, MSM8996, MSM8953, MSM8996, MSM896AU, MSM8953, MSM8996, MSM896AU, MSM8996, SDM630, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6- 031219/673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130		
			CVE ID : CVE-2019-2315		
sdm439_firm	ware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4- 031219/674

Weakness	Publish Date	cvss	C	Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated bound Auto, Selectron Snaped Snaped Snaped Mobile Music, Weara APQ80 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 QCN70 QM21 SDM4 SDM6 SDM7 SDX24 SM815	condition f resource concurried in the nent lead l access Snapdra onics Coloragon Idea (ragon Idea) (ragon Id	ce lock werently e memorish so our in Snape in Snape in Gornective onsume industria oT, Snape ragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905	which cpy t of dragon nsumer rity, er IOT, dragon roice & 19, 18, 7C, 19, 28, 7C, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Out-of- bounds Read	21-11-2019	10	while sessio messa un-int Snapd Snapd Snapd Snapd Snapd	parsing n manag ges if ne ended v ragon A ragon C ragon I ragon I ragon I e, Snapd	downlingement of the second se	onk OTA sends  , er IOT, el IOT, odragon	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	c, Snapdrables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MS 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3953, MS 3953, MS 3953, MS 300, SDM 45, SDM 45, SDM 45, SDM 45, SDM 45, SDM 50, SDX24 50, SM7 50, SM7 50, SM7	APQ800 Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 GM8909, MSM8937, GM8940, SM8976, MSM8976, MSM89, E300, SD 429, SD 429, SD 429, SD 429, SD 4429, S	18, 5, 7, 5, 40, 5, 17, 198, CS605, A660, M439, M632, M670, M850, 5, 8150, d_2016				
Improper Authenticati on	21-11-2019	10	allowan NAS m result bypas Snapo Snapo Snapo Snapo Mobil Music Weara	of integrals MODEI nessages into aut is of NAS dragon A dragon C dragon I dragon I e, Snapdr ables in A	M to acc s which thentica in outo, ompute onsume ndustria oT, Snap dragon V ragon	ept any can tion er IOT, al IOT, odragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch:	NCIIF	PC ID
			MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> SDM <sup>o</sup> SDA <sup>o</sup> SDM <sup>o</sup> SD	dragon_H 1130, SX	DM9205 DM9607 DM9625 MDM9645 MSM8909, MSM8937, SM8940, SM8976, MSM89 2150, Q0 30X, SDA 429, SDA 429, SDA 4660, SD	5, 7, 6, 40, 6, 40, 7, 7, 27, 28, 28, 28, 46, 46, 46, 46, 46, 46, 46, 46, 46, 46				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Micobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM600, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130  CVE ID : CVE-2019-2295  SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9640, MDM9150, MDM9640, MDM9506, MDM9640, MDM9655, MDM9640, MDM9655, MDM9640, MDM9655, MDM9640, MDM9650, MDM9640, MCM9640, MC	Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Voice				MSM8 MSM8 QCS44 SDA6 SDM6 SDM6 SDM6 SDM8 Snapo	3940, MS 3998, Nio 05, QCS6 60, SDA8 39, SDM 32, SDM 570, SDM 550, dragon_H	5M8953, cobar, Q 505, QM2 345, SDM 450, SD 5636, SD 5710, SD	CS404, 215, 4429, M630, M660, M845,				
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	out side it receive lessage. Snapdra dragon Indragon Indr	its bour res malfo in Snapo agon Cor onsume idustria oT, Snapo ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9605 DM9605 SM8909, MSM891 SM8937, SM8940, MSM891 SM8940, MSM891 SM8940, SM8976, MSM8940, MSM891 SM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976, MSM8940, SM8976,	ndary ormed dragon inpute, r IOT, l IOT, dragon foice & 9, 8, 5, 7, 7, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10	w.qual m.com pany/i ct- securit lletins ber-20	ty/bu /octo	-	
	CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2					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, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID: CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8909, MSM8917, MSM8940, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, SSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4- 031219/680

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			,	130, SX <b>D : CVE-</b>		315				
Out-of- bounds Read	21-11-2019	2.1	Trustimemo result Snapo	decure Kozone to o pry read into DO dragon A dragon C dragon M dragon W dragon W dragon W dragon W dragon W dragon W 3917, MS 3937, MS 3937, MS 3937, MS 3953, MS 396AU, 50, SDM4 dragon_H	do an ariwhich which we's in auto, connective consume adustria dobile, coice & More and a APQ80 (28096, IPQ8074), SM8940, GM8940, GM89	bitrary vill vity, r IOT, l IOT, fusic, 17, 4, 1439, d_2016	https://w.qualm.com pany/jct- securitelletins ber-20 bulleti	com l/com produ ty/bu /octo	0-QUA-3 031219	
sdm630_firm	ware									
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi result in Sna Snapo Snapo Snapo Mobil Music Wears APQ8	e process t messag tion is no ing into apdragon dragon C dragon I dragon I	ge, Valid ot met an infin a Auto, compute consume dot, Snap dragon V ragon APQ800 Q8053,	exit ite loop , r IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/i ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	-4 4-5 5-6		6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch.	NCIIP	CID
			MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> SC818 SC818 SDM <sup>o</sup> SDM <sup></sup>	9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 9650, MS 3905, MS 3998, MS 3976, MS 3976, MS 3976, MS 3976, SDM 50, SDM 50, SDM 50, SDM 51, SM615 50, SM815 1130, SX D: CVE-	DM9607 DM9625 MDM9655 SM8909, MSM8915 SM8953, SM8953, SM8953, S605, Q1 660, SD 6632, SD 6632, SD 6670, SD 6632, SD 6670, SD 6632, SD 6670, SD 6632, SD 6670, SD 6670, SD 6850, SM7 250, High_Me R2130	M215, A845, M450, M636, M710, X20, 150,				
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modified stater bound Auto, Electric Snape Mobil Music Wears APQ8 APQ8 MDM	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, 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,				//ww lcom n/com produ ty/bu /octo 019- n	0-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	cvss		Description	on & CVE	ID	Pat	tch	NCIIP	CID
				MSM3 MSM3 QCN7 QM22 SDM4 SDM6 SDM7 SDX2 SM81		5M8996. cobar, S405, Q0 60, SDA 1439, SD 1636, SD 1845, SD 50, SM7	AU, CS605, 845, M630, M660, X20,				
Improper Validation of Array Index	21.	-11-2019	4.6	occur to im array Auto, Electr Snape Snape Snape Snape APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 MSM8	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM896AU, MSM896AU, MSM8953, MSM896AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20				//ww lcom produ ty/bu /octo )19- n	0-QUA- 031219	
Buffer Copy without Checking	21	-11-2019	7.2	from sourc	If a bitmap file is loaded from any un-authenticated source, there is a possibility				//ww lcom n/com	O-QUA- 031219	
Size of Input				that the bitmap can			pany/	produ			
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7 7-8		8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
('Classic Buffer Overflow')			buffer Snapo	tially candragon Adragon Colragon Colragon Colragon Indragon Maragon Works APO (198, MD) (198, SDM)	w. in auto, ompute onnectivonsume dustria lobile, foice & MQ8096A M9205, MSM89 405, QCS 180X, Sim 150, SD 150, SM 1130, SX	, vity, or ity, or IOT, IOT, IOT, Music in U, 98, M636, M710, X24, 8150, IR2130	ct- securit lletins, ber-20 bulleti	/octo )19-		
Out-of- bounds Read	21-11-2019	7.5	P2P a handl mana Snapo Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377,				//ww .com ./com produ ty/bu /octo 119- n	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID: CVE-2019-2268		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Weile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDM6- 031219/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130		
			CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	0-QUA-SDM6- 031219/688

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch:	NCIIF	PC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape SDM6 SDM6 SDM6 SDM6 SDM8 Snape , SXR1	lragon_F	ress range the System to code. in the System to, ompute onnection on sume adustria folice & More and a APQ80 (28053, SM8905) (3845, SDM (450, SDM	ge sDBG , vity, or IOT, l IOT, fusic, 09, , CS404, 215, M429, M630, M660, M845, d_2016	https:/ w.qual m.com pany/j ct- securing lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Weara	P modul out side it receiv lessage. i Snapdra dragon C dragon Ic dragon Ic e, Snapd c, Snapdra	its bounges malfolin Snapon Coronsume adustria oT, Snapon Vagon APQ800	ndary ormed dragon mpute, er IOT, l IOT, edragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM7 SDX2 SM61 SM82 Snapo , SXR1	096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MI 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 3053, MS 3075, SDM 450, SDM 450, SDM 50, SDX24 50, SM7 50, Iragon_H 1130, SXI D: CVE-	DM9205 DM9607 DM9625 MDM964 DM9655 M8909, MSM891 SM8976, MSM8976, MSM89 2150, Q0 30X, SDA 429, SDI 660, SD 660, SD 6845, SD 650, SM	98, CS605, A660, M439, M670, M850, ,				
N/A	21-11-2019	7.2	copy to the Paran are from environment of Snapo	e invoking from fd of a secure be neters be om non somment. Snapdradragon Colragon Colragon Wolragon W	or local bouffer, eing popsecure in Snape onnectivonsume adustria lobile, foice & March 1980 (1980)	ouffer ulated dragon npute, vity, r IOT, l IOT,	https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
sdm660_firm	ware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6- 031219/692

2-3

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

Weakness	Publish Date	cvss	ı	Descriptio	on & CVE	ID	Pat	ch.	NCIIP	CID
			MSM8 MSM8 QCM2 SC818 SDM4 SDM6 SDM6 SDM8 SDX5! SM81 Snapo	3920, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDA 30, SDM 30, SDM 45, SDM 5, SM615 50, SM82 dragon_H	5M8953, 5M8996, cobar, S605, Ql 660, SD 6439, SD 6670, SD 6850, SD 50, SM72 250, High_Me R2130	M215, A845, M450, M636, M710, X20, 150,				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race of lack of will be modificated bound Auto, Electron Snaped Snaped Mobil Music Wears APQ8 MDM MDM MDM MSM8 MSM8 MSM8 MSM8 QCN7 QM21	condition of resource e concur fied in the ment lead d access in Snapdra conics Co dragon In dragon In dra	n due to ce lock verently e memo ds to out in Snapo agon Cor onsume dustria oT, Snap ragon Veragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM893 cobar, S405, Q0	the which apy tof dragon assumer ity, ar IOT, adragon oice & 19, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10	https:/w.qualm.com pany/jct- securif lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	0-QUA-9 031219	
				29, SDM 32, SDM	439, SD	M630,				

Weakness	Pu	blish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
					710, SDM 4, SM61 50	•	•				
				CVE I	D : CVE-	2019-1	0486				
Use After Free	21-	-11-2019	2.1	daem static freed in Sna Snape Snape Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61 SM82	fter free on shute object in from a rapdragon of dragon	down dunstance in Auto, compute connectificonsume ndustria oT, Snapplragon Vagon APQ800 Q8053, APQ809 GM8905 GM8905 GM8905 GM8939, GM8	te to getting places  , vity, er IOT, el IOT, edragon voice & 19, 18, 18, 19, 19, 19, 19, 19, 19, 19, 19, 19, 19	https://w.qualm.com pany/ct- securi lletins ber-20 bulleti	ty/bu /octo	0-QUA- 031219	
Improper Validation of Array Index	21-	-11-2019	4.6	occur to im array Auto,	of-bound in came proper v index in Snapdra conics Co	era drive ralidation Snapdr agon Cor	er due n of agon nsumer	https://w.qualm.com pany/ct-securi	com /com produ	O-QUA- 031219	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MSM8 MSM8 MSM8 MSM8 MSM8 SDX2		ndustria Jobile, Joice & M Vearable Q8017, Q8096A M9206, MDM9650 DM9650 MSM8937, MSM8937, MSM8937, MSM89	Music, es in U, 77, 77, 17, 17, 198, 10M450,	lletins ber-20 bulleti	19-		
Out-of- bounds Read	21-11-2019	4.6	Buffer in fast to impose while from Snape	D: CVE- r over-re t messag proper in process firmwar dragon A dragon C dragon I dragon I dragon W 053, AP 605, QC 60, SDM 0, SDX24	ead can of ge handle ing a mediato, consume industriand Mobile, coice & MORANS MOST MOST MOST MOST MOST MOST MOST MOS	occur er due idation essage er rity, er IOT, al IOT, Music in U, 198, CS605, M660,	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	ty/bu /octo n	0-QUA- 031219	
Buffer Copy without Checking	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility				https:/ w.qual m.com	com	0-QUA-	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Size of Input ('Classic Buffer Overflow')			poten buffer Snapo	he bitma tially cau tially cau dragon A dragon C dragon C dragon In dragon In dragon I dragon V 016, APC 098, MD 3996AU, ar, QCS4 55P, SC8 45, SDM 560, SDM 50, SM7 50, SXR1 D: CVE-	use stack w. in uto, ompute onnectiv onsume onsume dustria lobile, oice & M 28096A M9205, MSM89 05, QCS 180X, SI 630, SDI 670, SD 850, SD 150, SM	, vity, r ity, r IOT, l IOT, U, 98, 605, DA660, M636, M710, X24, 8150,	pany/j ct- securit lletins, ber-20 bulleti	ty/bu /octo 19-		
Out-of- bounds Read	21-11-2019	7.5	P2P a handl mana Snapo Snapo Snapo Snapo APQ8 APQ8 MDM MDM MSM8	ole OOB ction fra ing WLA gement f dragon C dragon C dragon Ir dragon Ir dragon V 009, APO 053, APO 098, MD 9207C, M 9650, MS	mes when North Nor	r ity, r IOT, l IOT, fusic in U, AU,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

QCA9379, QCS405, QCS605, SDA660, SDM636, SDM660, SDM630, SDM636, SDM670, SDM710, SDM845, SDX20, SM6150   CVE ID : CVE-2019-2268   Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Compute, Snapdragon Compute, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8098, MDM9150, MDM9607, MDM9206, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909, MSM8917, MSM8920, MSM8933, MSM8976, MSM8935, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8963, SDM636, SDM640,	Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	CID
Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9205, MDM9205, MDM9615, MDM9625, MDM9615, MDM9625, MDM9650, MSM8999, MSM8917, MSM8920, MSM8917, MSM8920, MSM8917, MSM8920, MSM8976, MSM8996AU, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM632, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016				SDA6 SDM6	60, SDM 660, SDM	630, SDI 1670, SD	M636, M710,				
While parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9205, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9650, MDM9655, MSM8909, MSM8999, MSM8917, MSM8920, MSM8917, MSM8920, MSM8917, MSM8920, MSM8998, Nicobar, QCM215, CC8160X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM632, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM632, SDM630, SDM630, SDM632, SDM630, SDM50, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016				CVE I	D : CVE-	2019-2	268				
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		21-11-2019	10	while session messar un-information of Snapor Snapo	parsing on manages if neitended with tended with tended with tended with tended with tended in the second of the s	downlingement of tworks alues in uto, ompute, onsume industria oT, Snap ragon Vagon APQ800 DM9605 DM9605 DM9605 DM9655 DM9605 DM9655 DM8940, SDM8940, SDM8976, MSM89 DM8976, DM865 D	nk OTA ends  r IOT, l IOT, dragon oice &  9,  8,  7,  40,  7,  27,  40,  6,  M439, M632, M670, M850,  8150,	w.qual m.com pany/i ct- securit lletins ber-20	com /com produ ty/bu /octo	•	
	CV Scoring Scal (CVSS)	e 0-1	1-2	<b>2-3</b> 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-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9640, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6- 031219/700

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	:ch	NCIIF	PC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape SDM6 SDM6 SDM6 SDM6 SDM8 Snape , SXR1	lragon_F	ress rang the Sys code. in uto, ompute, onnectiv onsume industria lobile, oice & M vired and APQ80 (8053, SM8905, SM8905, SM8937, SM8937, SM8937, SM8937, SM8953, cobar, Qu 2845, SDM 450, SD 450, SD 4710, SD	ge DBG  vity, r IOT, l IOT, 4usic, 09, , CS404, 215, 4429, M630, M660, M845, d_2016	https:/w.qualm.com pany/ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user s Auto, Electr Snapo Snapo Snapo Snapo Snapo	r overflo process ard NAN pace. in Snapdra conics Co dragon C dragon M dragon W dragon W	ing non- messag Snapdra gon Con onsume onsume dustria Iobile, oice & M	ge from agon asumer ity, r IOT, l IOT,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 APQ8 IPQ40 MDM' MDM' MSM8 QCA6 QCA9 QCS40 SDA8 SDM8		Q8053, Q8096A Q8096A, IP DM9207 DM9640 GM8905 QCA617 QCA937 N7605, O5, SDA 636, SDI 20, SDX	U, Q8074, C, , , , , , , , , , , , , , , , , ,				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear; APQ8 APQ8 MDM' MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8	P modul out side it received sage. it sages it s	e may active bounders malfolian Snapolian Snap	ccess idary ormed dragon inpute, r IOT, dragon oice &  9,  8,  7,  40,  7,  77,	https:/w.qualm.com pany/jct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-3 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	45, SDM 50, SDM 36, SDM 10, SDM 0, SDX24 50, SM7 50, dragon_H 1130, SX <b>D: CVE</b> -	1630, SD 1660, SD 1845, SD 1, SDX55 150, SM High_Me R2130	M632, M670, M850, 5, 8150, d_2016				
N/A	21-11-2019	7.2	copy to the Paramare from Environment of Snapor Sna	e invoking from fd of a secure of the comment. Snapdragon of the comment of the c	or local lebuffer, eing popsecure in Snapegon Consumendustria Mobile, Voice & More and a APQ80 Q8053, Q8096A Q805, QM9150, SM8909 Q805, SM8909 Q805, QM9150, SM8909 Q805, SM8909 Q805, SM8909 Q805, SM8909 Q805, QM9150, SM8909 Q805, SM8900 Q805, SM8900 Q805, SM8900 Q805, SM8900 Q805, SM89	buffer bulated dragon mpute, vity, er IOT, d IOT, U, 6, 09, U, 98, 215, M429, M630, M660, M845,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-3 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315		
snapdragon_h	 nigh_med_201	6_firm			
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	0-QUA-SNAP- 031219/705
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 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-2019-2335		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM630, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SNAP- 031219/706
Improper	21-11-2019	10	Lack of integrity check	https://ww	O-QUA-SNAP-
	i .		i	I	1

Weakness	Publish Date	cvss	[	Descriptio	n & CVE	Pat	ch	NCIIF	PCID	
Authenticati			allow	s MODEN	M to acc	ept any	w.qual	com	031219	9/707
on			NAS n	nessages	which	can	m.com	/com		
			result	into aut	hentica	tion	pany/j	produ		
				s of NAS			ct-			
			•	lragon A	•		securit			
				lragon C			lletins			
			•	lragon C		•	ber-20			
			_	lragon Ir			bulleti	n		
			_	lragon Io	•	•				
				e, Snapd	•	oice &				
				, Snapdr	•	0				
				ables in A	•	9,				
			ŭ	017, AP(	•	O				
				096AU, <i>I</i> 9150, MI	•	•				
				9130, MI 9206, MI						
				9615, MI						
			MDM9635M, MDM9640, MDM9650, MDM9655,							
				3905, MS						
				3909W, N	•					
				3920, MS		•				
				3939, MS						
				3953, MS						
				3996AU,						
			Nicob	ar, QCM	2150, Q	CS605,				
			QM21	5, SC818	30X, SDA	A660,				
			-	45, SDM						
			SDM4	50, SDM	630, SD	M632,				
			SDM6	36, SDM	660, SD	M670,				
			SDM7	10, SDM	845, SD	M850,				
			SDX20	), SDX24	, SDX55	,				
			SM61	50, SM7	150, SM	8150,				
			SM82	50,						
			Snapd	lragon_H	ligh_Me	d_2016				
			, SXR1	130, SX	R2130					
			CVE I	D : CVE-	2019-2	289				
Improper			Inforr	nation d	isclosur	e due	https:/	//ww		
Restriction	21-11-2019	2.1	to lacl	k of addr	ess rang	ge	w.qual	•	O-QUA-	-SNAP-
of	41-11-4019	2.1		done on			m.com		031219	9/708
Operations				s in SDI	•		pany/j	•		
CV Scoring Scale	9 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
within the Bounds of a Memory Buffer			Snapod Snapod Snapod Snapod Snapod Snapod Infras Netwo APQ8 MDM8 MSM8 MSM8 MSM8 QCS40 SDA60 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 Snapod SDM8 Snapod	lragon_H l 130 <b>D : CVE-</b>	Compute, Connective Consume Industria Mobile, Voice & Mobile, Voice & Mobile, Mobile, Mobile, Mobile, Mobile, Mobile, Mobile, Mobile, SM8937, SM8937, SM8953, Cobar, Quitable, SDM Mobile,	vity, or IOT, I IOT, Music, 09, , , CS404, 215, M429, M630, M660, M845, d_2016	ct- securit lletins, ber-20 bulleti	octo )19-		
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snape Snape Mobil Music Weara APQ8 APQ8 MDM9	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,				//ww lcom l/com produ ty/bu /octo 019- n	O-QUA-9	

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			MDM <sup>o</sup> MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	lragon_F l 130, SX	DM9655 M8909, MSM8915 M8940, MSM8976, MSM89 2150, Qu 30X, SDA 429, SDA 429, SDA 660, SD 660, SD 6845, SD 6845, SD 6845, SD 6845, SD 6845, SD 6845, SD	5, 17, 98, CS605, A660, M439, M632, M670, M850, 5,				
				D : CVE-						
N/A	21-11-2019	7.2	copy to the Paramare from Para	e invoking from fd of e secure he neters be om non so onment. Snapdra dragon C dragon In dragon W dragon W	or local louffer, eing popsecure in Snapegon Coronsumendustria lobile, eined and APQ80 Q8053, Q8096A M9150, DM9650	ouffer oulated dragon mpute, vity, or IOT, l IOT, dusic, U, o,	https:/ w.qual m.com pany/s ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			MSM8 MSM8 QCS4 SDA6 SDM6 SDM6 SDM8 SM81 Snapo	3917, MS 3937, MS 3953, MS 3996AU, 04, QCS6 60, SDA6 332, SDM 332, SDM 570, SM6 50, SM6 tragon_H 1130, SX <b>D: CVE-</b>	5M8940, 5M8996, MSM89 505, QM2 545, SDM 1450, SDM 1710, SDM 150, SM High_Me R2130	98, 215, 4429, M630, M660, M845, 7150,				
Out-of- bounds Read	21-11-2019	2.1	Trust memore result Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 APQ8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 Snapo	decure Kory read into DO dragon Adragon Coloragon Williagon Willia	do an ar which which we's in auto, donnecting donsume and white and a APQ80 Q8096, IPQ8074 GM8940, GM8940, QCA808	bitrary vill vity, r IOT, l IOT, fusic, 17, 4, 1439, d_2016	https:/ w.qual m.com pany/ ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-9 031219	
mdm9150_fir	mware		Han after free iggue in Vtra				1.44	1.1	0.0114	
Use After	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to			https:/ w.qual	•	O-QUA- MDM9-		
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	2-3 3-4 4-5 5-6				7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Descriptio	on & CVE	ID	Pat	ch	NCIIF	CID
Free			static freed in Snape Snape Snape Snape Snape Snape Snape Snape Mobil Music Wear; APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM8 SM61 SM82 CVE I	object ir from a mandragon Calragon Calragon Indragon Ind	nstance and the property of th	getting places vity, r IOT, l IOT, dragon oice &  9,  8,  7,  W,  AU, CS605, M450, M710, 24, 8150,	m.com pany/j ct- securit lletins ber-20 bulleti	produ ty/bu /octo 119-	031219	0/712
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Weara APQ8	P modul out side it receive essage. Snapdradragon Indragon Indrago	its bour res malfo in Snapo ngon Cor onsume ndustria oT, Snap ragon V ragon APQ800 Q8053,	ndary ormed dragon npute, r IOT, l IOT, dragon oice &	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303 While invoking the API to copy from fd or local buffer							
N/A	21-11-2019	7.2	copy to the Paramare from Environment of Snapo S		or local bouffer, eing popsecure in Snapeligon Coronsumendustria foice & March	ouffer oulated dragon npute, vity, r IOT, l IOT, dusic, 09,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- MDM9- 031219	/714
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
mdm9640_fir	mware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MDM9- 031219/715

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss		Description & CVE ID				ch	NCIIP	C ID
			MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	3940, MS 3976, MS 3998, Nie 150, QC 30X, SDM 30, SDM 60, SDM 5, SM61! 50, SM8 dragon_H 130, SX	5M8996. cobar, S605, Q 1660, SD 1632, SD 1670, SD 1850, SM7 250, High_Me R2130	AU, M215, A845, M450, M636, M710, X20, 150, d_2016				
				conditio						
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated bound Auto, Electron Snape Snape Mobil Music Wears APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6	f resour e concur ied in the nent lead d access Snapdra conics Codragon In dragon In dragon In dragon In dragon In 3968U, I 3969W, I 3998, Ni 3998, Ni 605, QC 5, SDA6 29, SDM 10, SDM	ce lock werently the memorals to our in Snapel agon Corrective consumer adustria oT, Snapel agon Veragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905 MSM	which  Tpy  t of dragon nsumer rity, er IOT, al IOT, odragon Toice &  19, 18, 7C, 19, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/716
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDX2- SM81	4, SM61! 50	50, SM71	150,				
			CVE I	D : CVE-	2019-1	0486				
Improper Validation of Array Index	21-11-2019	4.6	array Auto, Electr Snape Snape Snape Snape Snape APQ8 APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 MSM8	to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503  Improper validation for loop			https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/717
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improvarial firmw bound functi throu Auto, Snapo Snapo Snapo	oper vali vare can d access on while gh loop i Snapdra dragon C dragon C dragon M	dation for ved from lead to of in WLAI e iteration in Snapo in Sna	or loop out of N ng dragon npute, r ity, r IOT,	https:/ w.qual m.com pany/j ct- securing lletins ber-20 bulleti	com /com produ ty/bu /octo 119- n	O-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 APQ8 MSM8 QCA6 QCS4 SDM8	dragon V 053, AP 098, MD 3996AU, 574AU, 05, QCS 445, SDX <b>D: CVE-</b>	Q8096A M9640, MSM89 QCN760 605, SDA	U, 98, 5, 845,				
				r over re						
Out-of- bounds Read	21-11-2019	10	session messar un-interpretation of the session messar un-interpretation of the session of the s	parsing on manages if no tended with the dead of the d	gement etwork stalues in auto, sompute on sume adustria oT, Snap dragon Vagon APQ800 DM9607 DM9607 DM9607 DM9605 SM8909 MSM8937 MSM8940 MSM893 MSM8940 MSM893 MSM8940 MSM893 MSM8940 MSM893 MSM8940 MSM893 MSM8940 MSM893 MSM8940 MSM8	OTA ends ends r IOT, 1IOT, dragon oice & 9, 8, 7, 7, 140, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16	https:/ w.qual m.com pany/s ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/719
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Weakness	Publish Date	CVSS	SM61 SM82 Snapo , SXR1 CVE I Lack of allow NAS in result bypas Snapo Snapo	50, SM7	Iigh_Med R2130 <b>2019-2</b> Ity check M to accombinate of which of thenticate in uto,	8150, d_2016  271 k ept any can tion	Pat	ch	NCIIP	CID
Improper Authenticati on	21-11-2019	10	Snapo Snapo Mobil Musio Wears APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM7 SDX20	dragon Indragon Indragon Idragon Idrag	ndustria oT, Snap ragon V agon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9655 MB909, MSM891 SM8937, SM8940, SM8940, SM8940, SM8940, SM8976, MSM89 2150, QU 429, SDI 660, SD 660, SD	1 IOT, dragon foice & 9, 8, 5, 7, 6, 40, 5, 6, 4660, M439, M632, M670, M850, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- MDM9- 031219	/720
CV Scoring Scal	<u> </u>			lragon_F		d_2016				
(CVSS)	0-1	1-2	2-3	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-2019-2289		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MDM9- 031219/721
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MDM9- 031219/722
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303		
msm8909w_f	irmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/723

3-4

459

6-7

7-8

8-9

5-6

9-10

2-3

0-1

CV Scoring Scale

(CVSS)

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> SC818 SC818 SDM <sup>o</sup> SDM <sup></sup>	9150, MI 9206, MI 9615, MI 9635M, I 9650, MS 3905, MS 3909W, I 3920, MS 3940, MS 3976, MS 3976, MS 307, SDM 50, SDM 50, SDM 50, SDM 50, SDM 51, SM61S 1130, SX	DM9607 DM9625 MDM9655 MB9655 MSM8909, MSM8915 SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8975 SM8953, S	M215, A845, M450, M636, M710, X20, 150,				
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modified stater bound Auto, Electric Snape Mobil Music Wears APQ8 APQ8 MDM	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640,				//ww lcom l/com produ ty/bu /octo 019- n	0-QUA- MSM8- 031219	/724
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID: CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8917, MSM8939, MSM8940, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA645, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MSM8- 031219/725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM896AU, MSM8953, MSM896AU, MSM898, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/726
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA- MSM8- 031219/727

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>o</sup> MSM8 QCA9 SDM8 SM81	9206, MI 9607, MS 3909W, N 980, QCS 45, SDX 50 <b>D : CVE-</b>	5M8909 Nicobar, 5405, QC 24, SM7	, 2S605, 150,				
Out-of- bounds Read	21-11-2019	10	Buffer while session messar un-information of Snapor Snapo	r over reparsing on manages if new dragon Adragon College on Indiagon India	ad can he downling gement of tworks alues in uto, ompute, onsume adustria of, Snap ragon Vagon APQ800 Q8053, APQ809 QM9607 QM9607 QM9605 QM960	appen ak OTA ends or IOT, lot, dragon oice & 9, 8, 5, 40, 5, 440, 6, 4660, M439, M632, M670, M850, 6, 7, 100 M850, 7, 100 M850	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com orodu cy/bu /octo 19-	0-QUA- MSM8- 031219	/728
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	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, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9640, MDM9635M, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, SD845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SD	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130		
			CVE ID : CVE-2019-2289		
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2303	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA- MSM8- 031219/730

Weakness	Publish Date	CVSS	C	escriptio	n & CVE	Pat	ch	NCIII	PC ID	
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condition resulting in Snaped Snaped Snaped Snaped Mobile Music, Wear and APQ80 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SDX55 SM815 Snaped , SXR1	process messag ion is no ing into pdragor ragon C ragon Ic ragon Ic e, Snapdr bles in A 017, APC 096AU, A 0150, MI 0635M, I 0635M, I 0635M, I 0905, MS 0909W, M 0905, MS 0905,	re, Valid of met an infin in Auto, ompute onsume industria oT, Snap ragon Vagon APQ809 DM9607 DM9607 DM9605 SM8909, MSM891 SM8953, SM8	exit ite loop , er IOT, l IOT, dragon oice & e9, 8, 5, 40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150, d_2016	https:/w.qualm.company/jct-securitelletins/ber-20bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
Improper Restriction of Operations within the	21-11-2019	7.2	lack of array s image	bound a f check of ch	of whilte le readi nents. in	elist ng the	https:/ w.qual m.com pany/j	com /com	0-QUA- 031219	-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Bounds of a Memory Buffer			Snapo Snapo Snapo Snapo Infras Netwo QCS4 SDM6 SDM6 SM61 SXR1	dragon C dragon C dragon I dragon W dragon V dragon V tructure orking ir 04, QCS6 570, SDM 50, SM7 130, SXR	onnectionsumendustrial Mobile, Vired e and MDM9 M710, SD M710, SD M2150, SM	vity, er IOT, l IOT, 205, 845, M845, 55, 8150,	securit lletins ber-20 bulleti	octo 19-		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated bound Auto, Electron Snape Mobil Music Wears APQ8 MDM MDM MDM MSM8 MSM8 MSM8 MSM8 QCN7 QM21	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM896AU, MSM898, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630,				//ww .com ./com produ ty/bu /octo 019- n	0-QUA-0 031219	•
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909, MSM8909, MSM8909, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, SDA660, SDA660, SDA660, SDM670, SDM710, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130  CVE ID: CVE-2019-10490	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-QCS6- 031219/734
Improper Restriction of Operations within the Bounds of a Memory	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo	0-QUA-QCS6- 031219/735
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20  CVE ID: CVE-2019-10535	ber-2019- bulletin	
Out-of- bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8996AU, MSM8996AU, GCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24  CVE ID: CVE-2019-10563	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-QCS6- 031219/736
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-QCS6- 031219/737
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-QCS6- 031219/738

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130		
			CVE ID: CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-QCS6- 031219/739
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	0-QUA-QCS6- 031219/740
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			QCA9 SDA6 SDM6	574AU, ( 379, QCS 60, SDM 660, SDM 845, SDX	5405, Q0 630, SD 670, SD	CS605, M636, M710,				
			CVE I	D : CVE-	2019-2	268				
Out-of- bounds Read	21-11-2019	10	while session messar un-in Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	r over reparsing on manages if neaded with the design of t	downlingement of tworks alues in uto, ompute onsume industria of, Snap ragon Vagon APQ800 DM9605 DM9	nk OTA sends or IOT, I IOT, I IOT, Idragon oice & 9, 8, 5, 7, 6, 40, 6, 7, 17, 17, 17, 18, 17, 18, 18, 19, 19, 19, 19, 19, 19, 19, 19, 19, 19	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	•
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130		
			CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8953, SDM630, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6- 031219/742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130  CVE ID: CVE-2019-2295	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-QCS6- 031219/743
			Buffer overflow can occur while processing non-	https://ww	
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-QCS6- 031219/744

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS	1	Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			Infras Netwo APQ8 APQ8 IPQ40 MDM MDM MSM8 QCA6 QCA9 QCS4 SDA8 SDM8 SM81		and APQ80 Q8053, Q8096A B064, IP DM9207 DM9640 GM8905 QCA617 QCA937 N7605, O5, SDA 636, SDI 20, SDX2	U, Q8074, C, , , , , , , , , , , , , , , , , ,				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Musio Wear APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8	Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9615, MDM9635		https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	0-QUA- 031219	•	
CV Scoring Scale	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	ar, QCM .5, SC81; 45, SDM .50, SDM .36, SDM .10, SDM .50, SM7 .50, SM7 .50, .dragon_H .130, SX .dr. CVE-	80X, SDA 429, SDA 1630, SDA 1660, SDA 1845, SDA 150, SMA High_Me R2130	A660, M439, M632, M670, M850, S, 8150, d_2016				
N/A	21-11-2019	7.2	copy to the Paramare from Environment of Snapor Sna	e invoking from fd of secure lancers be om non a comment. Snapdra dragon of dragon of dragon vertice o	or local louffer, eing popsecure in Snapagon Consumendustria Mobile, Voice & More and APQ80 Q8053, Q8096A Q8053, Q8096A Q	buffer bulated dragon mpute, vity, er IOT, d IOT, U, 6, 09, U, 6, 108, 109, 109, 109, 109, 109, 109, 109, 109	https:/w.qualm.com pany/jct- securifiletins ber-20 bulleti	ty/bu /octo	O-QUA-031219	•
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM8 SM81 Snapd , SXR1	50, SM6 50, ragon_F 130, SX	710, SD 150, SM High_Med R2130 <b>2019-2</b> :	7150, d_2016				
Use After Free	21-11-2019	7.2	cleanumissir for a fapplic Comp Consul Indus Mobil Infras Netwo QCS40 SDX55 SM81	ng pointo ailed sta ation. in ute, Sna mer IOT trial IOT e, Snapd tructure orking in 04, QCS6 70, SDM 5, SM615	ne due to er sanitiz art of a tr Snapdr pdragon G, Snapdr G, Snapdr J, Snapdr	ragon ragon ragon ragon ragon ragon rired 205, 845, M845, .50, R2130	https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-031219	-
sdx20_firmwa	are									
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,		https:/ w.qual m.com pany/j ct- securit lletins	com /com produ ty/bu /octo	O-QUA-: 031219			
			APQ8 APQ8 MDM9 MDM9	ables in A 017, APO 096AU, A 0150, MI 0206, MI	APQ800 <sup>0</sup> Q8053, APQ8099 DM9205	3, , ,	ber-20 bulleti			

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9635M, I 9650, MI 3905, MS 3909W, I 3920, MS 3940, MS 3976, MS 2150, QC 30X, SDM 530, SDM 545, SDM 545, SDM 550, SM82 dragon_H	DM9655 M8909, MSM8916 M8937, M8953, M89966 Cobar, S605, Q1 660, SD 632, SD 670, SD 670, SD 850, SM72 250, High_Me	AU, M215, A845, M450, M636, M710, X20,				
				D : CVE-						
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modified stater bound Auto, Electric Snape Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MSM8	Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8052		https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219		
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID: CVE-2019-10486 Use after free issue in Xtra							
Use After Free	21-11-2019	2.1	daem static freed in Sna Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musio Wear APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61 SM82	fter free on shutd object in from a map dragon Chagon Chagon Indragon Indra	lown duastance grading in Auto, ompute, onnectivonsume adustria oT, Snapperagon Vagon APQ800 Q8053, APQ809 Q8053, APQ809 Q8053, GM8909 QSM8939, GM8939, GM8939	e to getting places  vity, r IOT, l IOT, dragon oice &  9,  8,  7,  W,  AU, CS605, M450, M710, 24, 8150,	https:/ w.qual m.com pany/i ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Improper Validation of	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due			https://ww w.qualcom		0-QUA- 031219		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIP	CID
Array Index			array Auto, Electr Snape Snape Snape Snape Snape APQ8 APQ8 APQ8 MDM MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8	index in Snapdra conics Co dragon C dragon M dragon W 009, APO 053, APO 098, MD 9207C, M 9640, MS 8905, MS 8920, MS 8920, MS 8940, MS 8940, MS 8940, MS 895, SDM 00	oice & M Vearable Q8017, Q8096AI	agon asumer ity, r IOT, l IOT, fusic, es in U, 7, 7, 7, M450, M660,	m.com pany/j ct- securit lletins ber-20 bulleti	cy/bu /octo		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	varial firmw bound functi throu Auto, Snapo Snapo Snapo Snapo APQ8	through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605,		https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ cy/bu /octo 19-	0-QUA-9 031219		
			MSM8 QCA6	3996AU, 574AU, (	MSM89	5,				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20		
			CVE ID : CVE-2019-10535		
Out-of- bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24  CVE ID: CVE-2019-10563	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDX2- 031219/753
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDX2- 031219/754
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDA8- SDM8	605, QC 45, SDM 45, SDX 50, SM8	670, SD 20, SM6	M710, 150,				
			CVE I	D : CVE-	2019-1	0566				
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150				https:/ w.qual m.com pany/ ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
			CVE I	D : CVE-	2019-2	268				
Out-of- bounds Read	21-11-2019	10	SDM845, SDX20, SM6150  CVE ID: CVE-2019-2268  Buffer over read can happen while parsing downlink session management OTA messages 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://w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	ables in 2 017, APC 096AU, 2 9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 3905, MS 3905, MS 3905, MS 3996AU, 45, SC818 45, SDM 45, SC818 45, SDM 450, SDM 50, SDX24 50, SM7 50, SM7	APQ800 Q8053, APQ809 DM9607 DM9605 MDM9655 SM8909, MSM8937, SM8940, SM8976, MSM89 2150, Q 80X, SDA 429, SDA 1630, SDA 1630, SDA 1650, SDA 150, SM	9, 8, 5, 40, 5, 40, 5, 40, 6, 6, 4660, M439, M632, M670, M850, 6, 8150, d_2016				
Improper Authenticati on	21-11-2019	10	CVE ID: CVE-2019-2271  Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	dragon_F 1130, SX	DM9607 DM9625 MDM9655 MB909, MSM8916 SM8940, SM8940, SM8940, SM8940, SM8956, MSM89 2150, Ql 80X, SDA 429, SDA 1660, SD 1845, SD 150, SM High_Me R2130	7, 40, 5, 40, 5, 17, 98, CS605, A660, M439, M670, M670, M850, 5,				
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	CVE ID: CVE-2019-2289  Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,			https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	/com /com produ ty/bu /octo	0-QUA- 031219		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 QCA6 QCA9 QCS4 SDA8	9650, MS 3996AU, 574AU, Q 379, QCS 05, QCS6 45, SDM 345, SDX 50	QCA617 QCA937 N7605, 05, SDA 636, SDI	74A, 7, .660, M660,				
			CVE I	D : CVE-	2019-2					
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modulout side it receives age. it sage. it sage. it sage it dragon I dragon, MI	its bour es malfo in Snapo gon Cor onsume dustria oT, Snap ragon V agon APQ809 DM9605 DM9605 DM9655 MDM9655 MB909, MSM891 EM8937, EM8940, EM8940, EM8940, EM8940, EM8940, EM8940, EM8940, EM8950, Que EM8950, Que EM8950, SD EM8950, SD	ndary ormed dragon inpute, in IOT, dragon oice & 9, 8, 5, 7, 7, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	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, Snapdragon_High_Med_20, , SXR1130, SXR2130	16	
			CVE ID : CVE-2019-2303		
sm7150_firm	ware				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite lo in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT Snapdragon Industrial IOT Snapdragon IoT, Snapdrag Mobile, Snapdragon Voice Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215 SC8180X, SDA660, SDA845 SDM630, SDM632, SDM636 SDM660, SDM670, SDM716 SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_20 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71- 031219/760
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6 6-7 7-8	8-9 9-10

Weakness	Pub	lish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID					
				CVE I	D : CVE-	2019-2	335									
Use After Free	21-7	11-2019	4.9	listen memo use af Snapo	•	result in uption d issue. in uto, compute connectionsume doustriand of the work of the wor	further ue to  , vity, er IOT, al IOT, Music, 205, 150, R2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219						
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-	11-2019	7.2	lack of array image Snapo Snapo Snapo Snapo Infras Network QCS40 SDM6 SM61	Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130		https:/ w.qual m.com pany/j ct- securing lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219							
Time-of- check Time- of-use	21-1	11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently				lack of resource lock which			lack of resource lock which		https:/ w.qual m.com	com	O-QUA-9	
CV Scoring Scal (CVSS)	е	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10					

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
(TOCTOU) Race Condition			stater bound Auto, Electr Snape Snape Snape Mobil Music Wears APQ8 MDM' MDM' MDM' MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX2- SM81		ds to ou in Snape igon Cor onnectiv onsume idustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM893 Cobar, S405, Q0 60, SDA (439, SD (636, SD (636, SD	t of dragon asumer rity, er IOT, al IOT, odragon roice & 19, 18, 17, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18	pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo 19-		
Use After Free	21-11-2019	2.1	CVE ID: CVE-2019-10486  Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SM71- 031219/765

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130		
			CVE ID: CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150  CVE ID: CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	0-QUA-SM71- 031219/766
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	0-QUA-SM71- 031219/767
CV Scoring Scal (CVSS)	e 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	tch	NCIIP	C ID
			MDM <sup>o</sup> MSM <sup>o</sup> Nicob QM21 SDA8 <sup>o</sup> SDA8 <sup>o</sup> SDM <sup>o</sup> SM <sup>o</sup>	lragon_H I 130, SXI	MDM96-55 M8909, MSM891 M8940, MSM8976, MSM89 2150, Q 80X, SD 429, SD 660, SD 6660, SD 6660, SD 150, SM	40, 5, 17, 98, CS605, A660, M439, M632, M670, M850, 5,				
Improper Authenticati on	21-11-2019	10	Lack of allow, NAS in result bypas Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM	Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,				//ww lcom n/com produ ty/bu /octo )19- n	0-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	lragon_F l 130, SX	MSM891 SM8937, SM8940, SM8976, MSM89 2150, Qu 30X, SDA 429, SDA 429, SDA 6660, SDA 6660, SDA 5660, SDA 5660, SMA Migh_Mea	98, CS605, A660, M439, M632, M670, M850, ,				
				<b>D : CVE-</b> P modul						
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8 MSM8	out side it receiv lessage. i Snapdra dragon C dragon Ic dragon Ic e, Snapdr ables in A 017, APC 096AU, A 9150, MI 9206, MI 9635M, I 9635M, I 3905, MS 3909W, I 3909W, I 3909W, I 3939, MS	its bour res malfo in Snapo gon Cor onsume dustria oT, Snap ragon V ragon APQ809 DM9205 DM9607 DM9625 MDM9655 SM8909, MSM891 SM8937, SM8940,	ndary ormed dragon npute, r IOT, l IOT, dragon oice &  9,  8,  6,  7,  40,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			Nicob QM21 SDA8 SDM4 SDM7 SDX20 SM61 SM82 Snapo	3996AU, ar, QCM; 5, SC818 45, SDM 50, SDM 10, SDM 10, SDM 50, SM7 50, SM7 51 130, SX D: CVE-	2150, Q0 30X, SDA 429, SDI 630, SD 660, SD 845, SD 5, SDX55 150, SM ligh_Me R2130	CS605, A660, M439, M632, M670, M850, 5, 8150,				
N/A	21-11-2019	7.2	copy for the the Paramare from	invokin from fd consecure is neters become non so onment. Snapdra Iragon Consecuration in Iragon Willington Willington Willington Willington Willington Willington in 19607, MI 19607, MI	or local bouffer, bing pope secure in Snape gon Coronsume dustria lobile, oice & More and a APQ80 (8053, Q8096A (M9150, QM9650, M8909, M8940,	ouffer oulated dragon mpute, vity, or IOT, l IOT, U, o,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9 031219	
l	i de la companya de			39, SDM	450. SD	MOSU.				

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDM8 SM81 Snapo	32, SDM 70, SDM 50, SM6 50, dragon_H 1130, SX <b>D: CVE-</b>	1710, SD 150, SM High_Me R2130	M845, 7150, d_2016				
				fter free		313				
Use After Free	21-11-2019	7.2	cleand missing for a fapplic Comp Consu Indus Mobil Infras Netwo QCS40 SDM6 SDX55 SM81	up routing points ailed state at a cation. in the cation i	ne due to er saniti ort of a to Snapdr pdragon T, Snapdo T, Snapdo Tagon W e and MDM9 105, SDA 1710, SD 1130, SX	zation custed ragon ragon vired 205, 845, M845, 150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-9 031219	
sxr1130_firm	ware									
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi result in Sna Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,				//ww .com ./com produ ty/bu /octo 119- n	O-QUA-9 031219	

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM6 SDX5 SM81 Snapo , SXR2	9615, MI 9635M, I 9635M, I 9650, MS 8905, MS 8920, MS 8940, MS 8976, MS 8998, Nic 2150, QC 80X, SDA 429, SDM 530, SDM 545, SDM 5, SM615 1130, SX D: CVE-	MDM9655 M8909, MSM8915 M8953, SM8953, SM8966, Cobar, S605, Q1 A660, SD A660, SD A670, SD A670	40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of lack of array image Snape Sna	f bound a of check of size white e elf segn dragon C dragon C dragon C dragon I dragon W dragon W structure orking ir 04, QCS6 570, SDM 550, SDX 50, SM7 130, SXR	access definition of the compute on sume on sum o	ue to elist ng the , vity, er IOT, 1 IOT, 205, 845, M845, 55,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Buffer Copy	21-11-2019	7.2	If a bitmap file is loaded					//ww	O-QUA-	SXR1-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
without Checking Size of Input ('Classic Buffer Overflow')			source that the potent buffer Snaped Snaped Snaped Snaped Snaped Snaped Snaped APQ80 MSM8 Nicobe SA615 SDA84 SDM6 SDM8 SM615 SM825 CVE II	any un-a e, there is te bitma tially cas toverflood ragon C dragon C dragon C dragon C dragon W dragon	is a possip can use stack w. in auto, ompute onnectivonsume onsume onsum	sibility k  vity, or ity, l IOT, l IOT, Music in U, 98, 605, DA660, M710, X24, 8150, ER2130	w.qual m.com pany/j ct- securit lletins ber-20 bulleti	/com produ ty/bu /octo	031219	/774
Out-of- bounds Read	21-11-2019	10	while session messan un-interpretation Snaped Snaped Snaped Mobile Music Weara APQ86 APQ86	rover reparsing namanages if nemed with the contraction of the contrac	downlingement of the setwork s	or IOT, I IOT, I IOT, I or Ioe &  9,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness Publish Date 0	cvss	[	Description	n & CVE	ID	Pat	ch	NCIIP	CID
		MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapd , SXR1	9206, MI 9615, MI 9635M, I 9650, MI 905, MS 9909W, I 8920, MS 8939, MS 8939, MS 8939, MS 8953, M	DM9625 MDM964 DM9655 M8909, MSM891 SM8937, SM8976, MSM89 2150, Q0 30X, SDA 429, SDI 630, SD 660, SD 845, SD 150, SM	98, CS605, A660, M439, M670, M850, ,				
Improper Authenticati 21-11-2019 on	10	allows NAS n result bypas Snapd Snapd Snapd Snapd Snapd Mobil Music Weara APQ8	of integrics MODENtessages into autorists of NAS ragon Caragon Caragon Integration Integra	M to accombined to accombine the second to accombine t	ept any can tion r IOT, l IOT, dragon oice &	https://w.qual m.com pany/s ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA-9 031219	
		MDM9	9150, MI 9206, MI 9615, MI 9635M, I	DM9607 DM9625	, , ,				

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM3 MSM3 MSM3 MSM3 MSM3 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	9650, MI 3905, MS 3909W, NS 3920, MS 3939, MS 3953, MS 3996AU, bar, QCM 15, SC818 45, SDM 450, SDM 710, SDM 710, SDM 50, SM7 50, SM7 150, SM7	SM8909, MSM8915, SM8940, SM8976, MSM89 2150, Q 80X, SD 429, SD 6630, SD 6660, SD 845, SD 8, SDX55 150, SM	98, CS605, A660, M439, M632, M670, M850,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information lack check buffer Snape	D: CVE- mation d k of addr done on rs in SDI dragon C dragon C dragon C dragon W dragon W dragon W structure orking in 017, APC 9205, MS 8909, MS 8940, MS 8998, Nic 05, QCS6 60, SDA8	isclosures range the System on the System on the System on sume on sume on sume on sume on the System on System on the System on	re due ge sDBG  vity, er IOT, l IOT,  Music,  CS404, 215,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDM6 SDM8 Snapo , SXR1	dragon_F	1636, SD 1710, SD High_Me	M660, M845, d_2016				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	P modulout side it receive essage. Snapdra dragon Idragon Idra	e may actives malforin Snapor Corsonsume adustria oT, Snapor APQ800 Q8053, APQ809 DM9605 DM8909 DM9605 DM8909 DM9605 DM8909 DM9605 DM8909 DM9605 DM8909 DM800	ccess ndary ormed dragon npute, r IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, 40, 6, 40, 6, 40, 6, 40, 6, 8150, 8150,	https:/w.qualm.company/jct-securifiletinsber-20bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			CVE ID: CVE-2019-2303  While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,		
			While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,		
			copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,		
N/A 2	21-11-2019	7.2	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, MSM8953, MSM8996, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	0-QUA-SXR1- 031219/779
Use After Free 2	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization	https://ww w.qualcom m.com/com	O-QUA-SXR1- 031219/780
CV Scoring Scale	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			applic Comp Consu Indus Mobil Infras Netwo QCS4 SDM6 SDX5 SM81	failed stacation. in oute, Sna oute, Sna outrial IOT e, Snapd structure orking in 04, QCS6 570, SDM 5, SM61! 50, SXR	i Snapdr pdragon C, Snapdi Iragon W e and i MDM9 505, SDA 1710, SD 50, SM7	ragon ragon ragon Vired 205, .845, M845, 150, .R2130	pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo )19-		
sdx24_firmwa	are									
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	lack of array image Snape Snap	f bound of check of size white elf segn dragon of dragon	of whilted ile readinents. in auto, auto, auto, auto, auto, auto, auto, auto, auto, auto auto auto auto auto auto auto auto	elist ng the vity, r IOT, l IOT, 845, 845, 845,	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer				https://w.qualm.com pany/jct-securit	com /com produ	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[	Descriptio	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81	ronics Colragon Colragon In Iragon Ir	onsumendustria oT, Snap dragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM893 GM8996, GOBAR, S405, QO 60, SDA (439, SD (636, SD (636, SD	r IOT, l IOT, dragon oice & 9, 8, 7C, 0, , 89, AU, CS605, 845, M630, M660, X20,	ber-20 bulleti			
Use After Free	21-11-2019	2.1	daeme static freed in Sna Snape Snape Snape Snape Snape Mobil Music Weara APQ8 APQ8 MDM9	cter free on shute object in from a mapped of the free	lown dunstance grantiple in Auto, ompute, onnection on Sume in Auto, on Sume in Auto, Snap in Appublication Vagon Vagon Appublication Vagon Va	e to getting places  vity, r IOT, dragon oice &  9,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	/com /com produ ty/bu /octo	O-QUA- 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM8 SM61 SM82	3909, MS 3917, MS 3937, MS 3940, MS 3998, Nio 60, SDM 45, SDX 50, SM7 50, SXR2	5M8920, 5M8939, 5M8953, 5M8996, cobar, Q 345, SDM 1670, SD 20, SDX 150, SM 2130	AU, CS605, 1450, M710, 24, 8150,				
Out-of- bounds Read	21-11-2019	4.6	in fast to imp while from: Snapo Sna	r over-ret message proper in process firmwardragon Adragon Coloragon Indragon Williagon Williago	ge handle ing a me e in tuto, consume consume dobile, voice & M Q8096A MSM89 S405, Q0	er due idation essage r ity, r IOT, l IOT, l IOT, 98, CS605, M660,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	/com /com produ ty/bu /octo	O-QUA-: 031219	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from source that the potent buffer Snape Snape Snape	tmap file any un-a e, there he bitma tially car overflo dragon A dragon C dragon C	nuthentions a possess ap can use stack w. in tuto, compute connectives	cated ibility k	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	O-QUA-: 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch:	NCIIP	C ID	
			Snapo Snapo Snapo APQ8 APQ8 MSM8 Nicob SA61: SDA8 SDM6 SDM6 SM61 SM82	ronics Co dragon O dragon M dragon V 016, APO 098, MD 3996AU, ar, QCS4 55P, SC8 45, SDM 660, SDM 50, SM7 50, SXR2	fonsume ndustria Mobile, Moice & M Q8096A M9205, MSM89 MO5, QCS 180X, SI 1670, SD 1850, SD 150, SM	Pr IOT, I IOT, I IOT, Music in U, 98, 6605, DA660, M636, M710, X24, 8150, (R2130					
				ole doub							
Use After Free	21-11-2019	4.6	kerne camer modu Snapo Snapo Snapo Mobil Musio Wear Wired Netwo IPQ40 MDM MDM MSM8 QCA9 SDM8 SM81	l while he ra senso les powedragon Adragon Idragon Idrastro 19, IPQ6 19206, MI 1980, QC 1980, Q	nandling r and its er seque auto, consume ndustria oT, Snap lragon lapdrago ructure a n APQ80 8064, DM9207 SM8909 Nicobar, S405, Q0	the sub ence in or IOT, odragon foice & on and 53,	https:/w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	O-QUA- 031219		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink				while parsing downlink w.qualcom $0.004-302$		w.qualcom		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIII	PC ID
			messa	ages if ne	twork s	ends	pany/	produ		
			un-in	tended v	alues in		ct-			
			Snapo	dragon A	uto,		securi	ty/bu		
			_	dragon C	•		lletins			
			Snapo	dragon C	onsume	r IOT,	ber-20			
			Snapo	dragon Ir	idustria	l IOT,	bulleti	n		
			_	dragon Io	•	O				
				e, Snapd	_	oice &				
				, Snapdr	•					
				ables in A	•	9,				
			~	017, APC	•					
			ŭ	096AU, A	•	•				
				9150, MI		•				
				9206, MI		•				
				9615, MI		•				
				9635M, I						
				9650, MI		•				
				3905, MS						
				3909W, N		•				
				3920, MS						
				3939, MS	•					
				3953, MS						
				3996AU,						
				ar, QCM: .5, SC818						
			_	45, SDM						
				45, SDM ∕50, SDM	•	•				
				36, SDM	•	•				
				'10, SDM	•	•				
				10, SDM 0, SDX24	•	•				
				50, SM71						
			SM82		130, 31410	0130,				
				dragon_H	ligh Me	d 2016				
			_	1130, SXI	_	u_2010				
				D : CVE-		271				
							https	/ /*****		
				of integri s MODEN	•		https:/ w.qual	•		
Improper							m.com		O-QUA-	SDX2-
Authenticati	21-11-2019	10	NAS messages which can result into authentication					produ	031219	
on			bypass of NAS in					produ		, : 00
				dragon A			ct- securit	tv/bu		
CV Scoring Scal	e 0.4	1.3				F.C.			0.0	0.10
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Snapo Snapo Snapo Mobil Musio Wear APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	dragon C dragon I dragon I dragon I dragon I de, Snapdr ables in I 017, APC 096AU, I 9615, MI 9635M, I 9635M, I 9635M, I 9635M, I 9635M, I 9635, MS 3905, MS 3005, SDM 450, SD	onsume industria oT, Snap Iragon V ragon APQ800 Q8053, APQ809 DM9625 MDM9655 MB9655 MB965 MSM8916, MSM8976, SDM8429, SDM	r IOT, l IOT, dragon foice & 9, 8, 5, 40, 5, 40, 5, 47, 40, 5, 40, 6, M439, M632, M670, M850, 7, 8150,	lletins, ber-20 bulleti	19-		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,				https://w.qual m.com pany/j ct- securit lletins/ ber-20	/com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					ch	NCIIP	C ID
			Snapo Infras Netwo APQ8 APQ8 IPQ40 MDM MDM MDM MSM8 QCA6 QCA9 QCS4 SDA8	dragon V dragon W structure orking in 017, APO 064, APO 965, IPQO 9650, MI 9650, MI 379, QCI 05, QCS6 45, SDMO 845, SDMO 50	Vired and APQ80 Q8053, Q8096A B064, IP DM9207 DM9640 SM8905 QCA617 QCA937 N7605, 505, SDA	09, U, Q8074, C, , , , , , , , , , , , , , , , , ,	bulleti	n		
				D : CVE-						
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8939, MSM8937, MSM8939, MSM8940, MSM8939, MSM8940, MSM8953, MSM8976,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	0-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2303		
Schneider-ele	ectric		CVE ID . CVE-2019-2303		
bmx_p34x_fir					
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.  CVE ID: CVE-2019-6852	https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019- 281-02/	O-SCH-BMX 031219/791
bmx_noe_010	0_firmware				
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium	https://ww w.schneider - electric.com /ww/en/do wnload/doc	O-SCH-BMX 031219/792
CV Scoring Scal (CVSS)	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID				Pat	ch	NCIIP	C ID
			Quant comm see se specif could FTP h when of the unsec	nunication tum CPU nunication curity n ic version cause the ardcode using the controll ure netv	s, Quant on modu otifications), who de disclo de creden de Web s der on ar vork.	tum les - on for ich sure of ntials erver	ument D-201 281-02	9-		
bmx_noe_011	0_firmware									
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.			https://w.schm- electrice/ww/e wnload ument D-2019 281-02	c.com en/do d/doc /SEV 9-	O-SCH-I 031219		
bmx_noc_040	1_firmware									
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules -			https://w.schm- electric /ww/e wnload ument D-2019 281-02	c.com en/do d/doc /SEV 9-	O-SCH-I 031219	_	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				ch	NCIIP	CID
tsx_p57x_firm	ware.		see securit specific ver could caus FTP hardco when using of the cont unsecure re	rsions), whe the disclost ded crede g the Web stroller on an etwork.	ich sure of ntials server				
tsx_ps/x_mm	lwai c		A CIME 20	) I	<u>.</u>			T	
Information Exposure	20-11-2019	5	Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules -		https:/ w.schr - electri /ww/e wnload ument D-201 281-02	c.com en/do d/doc /SEV 9-	O-SCH-' 031219		
tsx_ety_x103_	firmware								
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of			https://w.schr electri /ww/e wnload ument D-2019 281-02	c.com en/do d/doc /SEV 9-	O-SCH- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			FTP hardcoded credentials when using the Web server of the controller on an unsecure network.  CVE ID: CVE-2019-6852		
140_cpu6x_fii	rmware		CVE ID: CVE-2019-0852		
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.  CVE ID: CVE-2019-6852	https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019- 281-02/	O-SCH-140 031219/797
140_noe_771x	x1_firmware				
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an	https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019- 281-02/	O-SCH-140 031219/798
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 511	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			unsecure network.		
			CVE ID: CVE-2019-6852		
140_noc_78x0	00_firmware				
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.  CVE ID: CVE-2019-6852	https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019- 281-02/	O-SCH-140 031219/799
140_noc_7710	 01 firmware		0.2.2.0.2.2027		
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.  CVE ID: CVE-2019-6852	https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019- 281-02/	O-SCH-140 031219/800

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
ztehome			L							
c520v21_firm	ware									
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-11-2019	5	permission and access control vulnerability, which exists in V2.1.14 and below versions of C520V21 smart camera devices. An attacker can construct a URL for directory traversal and access to other unauthorized files or resources.  CVE ID: CVE-2019-3423  http://supp ort.zte.com. cn/support /news/Loo pholeInfoD etail.aspx?n ewsId=101 1842				.com. oport /Loo nfoD spx?n	O-ZTE-0 031219		
Improper Authenticati on	18-11-2019	6.4	authentication issues vulnerability, which exists in V2.1.14 and below versions of C520V21 smart camera devices. An attacker can automatically obtain access to web services from the authorized browser of the same computer and perform operations.			http://ort.zte cn/sup /news pholeI etail.as ewsId: 1842	.com. oport /Loo nfoD spx?n	0-ZTE-0 031219		
				Hardwa	are					
Lenovo										
thinkpad_usb	-c dock									
N/A	20-11-2019	5	A potential vulnerability reported in ThinkPad USB-C Dock Firmware version 3.7.2 may allow a denial of service.  CVE ID: CVE-2019-6176		N/A		N/A H-LEN-THI 031219/80			
thinkagile_7x	82									
Improper Neutralizatio n of Special Elements in	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could			orted	N/A		H-LEN-' 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6			5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pato	h	NCIIP	CID
Output Used by a Downstream Component ('Injection')			allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187				
thinkagile_7y	 <sub>'</sub> 11		CVE ID: CVE-2019-0107				
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187	N/A		H-LEN-7 031219	
thinkagile_7y	12		A stand CCV Inication			l	
Improper Neutralizatio n of Special Elements in Output Used by a Downstream	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store	N/A		H-LEN-7 031219	
CV Scoring Scal (CVSS)	le 0-1	1-2	<b>2-3 3-4 4-5 5-6 514</b>	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descript	ion & CVE	ID	Pat	ch	NCIIP	CID
Component ('Injection')			malformed d XCC server ir fields, that co crafted forms stored in an e file. The craft not executed and has no ef server.  CVE ID : CVE						
thinkagile_7y	<b>88</b>								
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.		N/A		H-LEN- 031219		
thinkagile_7y	92								
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV vulnerability in Lenovo XC Controller (X allow an admother appropermissioned malformed d XCC server in fields, that co	N/A		H-LEN- 031219			
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	D	escriptio	on & CVE	ID	Pat	ch	NCIII	PC ID
			stored file. Th not exe and ha server.	crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187						
thinkagile_7z	03									
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulners in Lence Contro allow a other a permis malfor XCC se fields, t crafted stored file. Th not exe and ha server.	ability volve XClored an administration and executed controls on effect of the controls of the control of the c	CC) that inistrati	could ve or store rtain onal lt in g CSV ula is stself the	N/A		H-LEN- 031219	
thinksystem_	sd530									
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is				N/A		H-LEN- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	l	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187							
thinksystem_s	sd650									
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulne in Ler Contr allow other permi malfo XCC s fields crafte store file. T not ex and h serve:	red CSV I rability value of XCI oller (XCI) an admit appropriates oned red da erver informed din an extent din din din din din din din din din din	was reported formation XCC in the contract of	could ve or store tain onal It in g CSV ula is tself	N/A		H-LEN-7 031219	
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulne in Ler Contr allow other permi malfo XCC s fields crafte stored file. T not ex	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the					H-LEN-7 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	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-2019-6187									
thinksystem_	sn850				1							
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187	N/A	H-LEN-THIN- 031219/813							
thinksystem_	sr150											
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187	N/A	H-LEN-THIN- 031219/814							
thinksystem_	sr158											
		thinksystem_sr158										

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulne in Ler Contr allow other permi malfo XCC s fields crafte store file. T not ex and h serve:	red CSV I rability v novo XCI oller (XC an admi appropri issioned rmed da erver inf that cou d formu d in an ex he crafte xecuted c as no eff r. D: CVE-	was reported for XCC in XCC in XCC in the test on the	could ve or store rtain onal It in g CSV ula is tself	N/A		H-LEN-7 031219	
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulne in Ler Contr allow other permi malfo XCC s fields crafte stored file. T not ex and h serve:	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187					H-LEN-7 031219	
thinksystem_	sr258									
Improper Neutralizatio n of Special	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity				N/A		H-LEN-7 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6		5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	1	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.			
thinksystem_	sr850		CVE ID . CVE-2019-0107			
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187	N/A		H-LEN-THIN- 031219/818
thinksystem_	sr860					
Improper Neutralizatio n of Special Elements in Output Used by a	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately	N/A		H-LEN-THIN- 031219/819
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIIPC ID
Downstream Component ('Injection')			permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187			
thinksystem_	st250					
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187	N/A		H-LEN-THIN- 031219/820
thinksystem_	st258					
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational	N/A		H-LEN-THIN- 031219/821
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pat	ch	NCIII	PC ID
			crafte stored file. The not extend has and has server	d formu I in an e he crafte ecuted as no eff	tat could result in Formulas being an exported CSV crafted formula is tuted on XCC itself no effect on the					
thinkagile_7d	1h									
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulner in Len Contra allow other permi malfo XCC so fields, crafte stored file. Th not ex and ha server	red CSV rability rabi	was reparity  CC) that inistratively user to ata in cert formatic uld resu las bein ed forme on XCC if fect on to	could ve or store rtain onal lt in g CSV ula is tself he	N/A		H-LEN- 031219	
thinkagile_7x	83									
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV				N/A		H-LEN- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIIPC ID
			file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187			
thinkagile_7y	13		012121012 <b>2</b> 017 0107			
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187	N/A		H-LEN-THIN- 031219/824
thinkagile_7y	14					
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the	N/A		H-LEN-THIN- 031219/825
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 523	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			server.		
			CVE ID : CVE-2019-6187		
thinkagile_7y	90				
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187	N/A	H-LEN-THIN- 031219/826
thinkagile_7y	93				
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187	N/A	H-LEN-THIN- 031219/827

CV Scoring Scale	0-1	1_2	2-3	2-1	4-5	5-6	6-7	7_8	<b>2</b> _0	0_10
(CVSS)	0-1	1-2	2-3	3-4	4-3	3-0	6-7	7-8	0-3	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIF	CID
thinkagile_7y	94									
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulner in Len Contro allow other permi malfor XCC se fields, craftee stored file. Th not ex and ha server	ed CSV Is rability woo XClandler (XC) an admination appropriation of that could formulate that could formulate crafted as no effective of the cours of the crafted of the cours of the cour	was reported formuted	could ve or store rtain onal lt in g CSV ula is tself	N/A		H-LEN-THIN- 031219/828	
thinkagile_7z	04		GVET	D. GVE	2017 0	107				
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulner in Len Contro allow other permi malfor XCC se fields, craftee stored file. Th not ex and ha server	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187		N/A		H-LEN- 031219		
thinkagile_7z	05									
Improper Neutralizatio	20-11-2019	4	A stored CSV Injection vulnerability was reported				N/A		H-LEN- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Descript	ion & CVE	ID	Pat	tch	NCIIP	CID
n of Special Elements in Output Used by a Downstream Component ('Injection')			in Lenovo XC Controller (X allow an admother appropriate of the controller of the co	CCC) that ninistrative or ately duser to lata in cere or ately ulas being exported ted formula for XCC iffect on the late of t	store stain onal lt in g CSV ula is tself				
thinkagile_7z	06		CVL ID I CVL	20170	107				
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187		N/A		H-LEN-' 031219		
thinkagile_7z	07								
Improper Neutralizatio n of Special Elements in Output Used	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or						
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIF	CID
by a Downstream Component ('Injection')			perm malfo XCC s fields crafte stored file. T not ex and h serve	approprissioned rmed da erver informula din an executed cas no efformula so the crafted cas no	user to ta in cer formation ald resur las bein exported ed formut on XCC i ect on the	tain onal It in G CSV ola is tself ne				
thinkagile_7z	20									
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulne in Ler Contr allow other perm malfo XCC s fields crafte store file. T not ex and h serve	ACC server informational   N/A		H-LEN- 031219				
thinkagile_yx	84									
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain				N/A		H-LEN- 031219	
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE I	D Pat	tch	NCIIP	CID
('Injection')			XCC server information fields, that could result crafted formulas being stored in an exported of file. The crafted formulation of executed on XCC it and has no effect on the server.  CVE ID: CVE-2019-61	t in CSV la is self			
thinksystem_	sr530						
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that callow an administrative other appropriately permissioned user to smalformed data in cert XCC server information fields, that could result crafted formulas being stored in an exported of file. The crafted formulant executed on XCC it and has no effect on the server.  CVE ID: CVE-2019-61	could re or store tain nal N/A t in CSV la is self e		H-LEN-7 031219,	
thinksystem_	sr550						
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that callow an administrative other appropriately permissioned user to smalformed data in certa XCC server information fields, that could result crafted formulas being	could le or N/A store tain nal t in		H-LEN-7 031219,	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description	on & CVE	ID	Pat	ch	NCIIP	PC ID
thinksystem_	sr570		stored in an efile. The crafte not executed and has no efficiency.  CVE ID : CVE	ed formu on XCC it fect on th	lla is tself ie				
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV vulnerability in Lenovo XCl Controller (XC allow an admother appropriate of the controller of the controlle	was reportantly  CC) that of the contraction in certain in certain certain certain in certain	orted could ve or store tain nal t in GCSV cla is cself	N/A		H-LEN- 031219	
thinksystem_	sr590								
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV vulnerability in Lenovo XCl Controller (XC allow an adm other appropriate permissioned malformed da XCC server in fields, that corrected formulations are file. The crafted not executed	N/A		H-LEN- 031219			
CV Scoring Scal	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			serve	as no eff r. <b>D : CVE-</b>						
thinksystem_	sr630		CVLI	DIGVE	2017 0	107				
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulne in Ler Contr allow other perm malfo XCC s fields crafte store file. T not ex and h serve	red CSV in rability in ovo XCI foller (XCI) an admit appropriate appropriate in the craft of the	was reportantly (CC) that inistrative user to late in certiformatic las being ed formution XCC in fect on the late of	could ve or store rtain onal It in g CSV ula is tself ne	N/A		H-LEN-7 031219	
thinksystem_	sr650									
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulne in Ler Contrallow other perm malfo XCC s fields crafte stored file. T not exand h serve	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187					H-LEN-7 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID				
thinksystem_	st550													
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187				in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.		Inerability was reported Lenovo XClarity Introller (XCC) that could ow an administrative or her appropriately rmissioned user to store alformed data in certain IC server informational Ids, that could result in afted formulas being ored in an exported CSV e. The crafted formula is of executed on XCC itself d has no effect on the rver.				H-LEN-' 031219	
thinksystem_	st558		CVLI	D.CVL	2017 0	107								
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	vulne in Ler Contr allow other perm malfo XCC s fields crafte store file. T not ex and h serve	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187			N/A		H-LEN-' 031219					
_thinksystem	_sr670													
Improper Neutralizatio	20-11-2019	4	A stored CSV Injection vulnerability was reported			N/A		H-LEN- 031219						
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10				

Weakness	Puk	olish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID			
n of Special Elements in Output Used by a Downstream Component ('Injection')				Contrallow other perm malfo XCC s fields crafte stored file. To not example and has serve	in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187									
thinksystem_	sr95	0		CVEI	D. CVE	2017 0	107							
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-	11-2019	4	vulne in Ler Contrallow other perm malfo XCC s fields crafte store file. T not example and h serve	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.  CVE ID: CVE-2019-6187					H-LEN-' 031219				
Linksys														
velop_whw03 Authorizatio	303			Polls:	n Linkov	c Volon								
n Bypass Through User-	21-	11-2019	6.4	1 1 0 102/10 devices allows		remote attackers to discover			1.1.8.192419 devices allows remote attackers to discover				H-LIN-V 031219	
CV Scoring Scal (CVSS)	le	0-1	1-2	2-3	2-3 3-4 4-5 5-6		6-7	7-8	8-9	9-10				

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
Controlled			_	st for the						
Key				fo_json. <b>D : CVE-</b> :	_	6240				
volon whw02	202		CVEII	D: CVE-	2019-1	0340				
velop_whw03	50Z		D 11:	Linksys	77.1					
Authorizatio n Bypass Through User- Controlled Key	21-11-2019	6.4	1.1.8.192419 devices allows remote attackers to discover the recovery key via a direct request for the /sysinfo_json.cgi URI.  CVE ID: CVE-2019-16340				N/A		H-LIN-V 031219	
velop_whw03	801									
Authorizatio n Bypass Through User- Controlled Key	21-11-2019	6.4	Belkin Linksys Velop 1.1.8.192419 devices allows remote attackers to discover the recovery key via a direct request for the /sysinfo_json.cgi URI.  CVE ID: CVE-2019-16340				N/A		H-LIN-V 031219	
phicomm										
k2\(psg1218	<i>\</i> )									
Improper Input Validation	18-11-2019	9	/admi PHICO V22.5 remot to exe shell r cgi-bii param	/usr/lib/lua/luci/controller /admin/autoupgrade.lua on PHICOMM K2(PSG1218) V22.5.9.163 devices allows remote authenticated users to execute any command via shell metacharacters in the cgi-bin/luci autoUpTime parameter.  CVE ID: CVE-2019-19117			N/A		H-PHI-k 031219	
Qualcomm										
mdm9206										
Loop with Unreachable Exit Condition	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop			https://ww w.qualcom m.com/com pany/produ		MDM9- 031219/849		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIF	PCID
('Infinite Loop')			in Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SDM4 SDM6 SDM6 SDM6 SDM6 SDM8 SDX58 SM81 Snapo	apdragor Clragon Clragon Clragon Idragon Idragon, MI 19635 M, Idragon, MI 19635 M, Idragon, SDM 1960, SDM	n Auto, ompute onsume onsume of the consume of the	r IOT, l IOT, dragon oice & 9, 8, 6, 7, 40, 6, 40, 6, M215, A845, M450, M636, M710, X20, 150,	ct- securit lletins ber-20 bulleti	ty/bu /octo 119-		
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack o will be modif staten bound Auto, Electr	condition f resource e concur fied in the nent lead d access Snapdra conics Co dragon C	ce lock verently se memods to out in Snapologon Corponnective	which  py t of dragon asumer ity,	https://w.qualm.com pany/jct- securit lletins/ ber-20	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			Snapo Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81		oT, Snap ragon V ragon APQ800 Q8053, APQ809 DM9640 SM8905 MSM896 Cobar, S405, Q0 60, SDA (439, SD (636, SD (845, SD	dragon foice & 9, 8, 7C, 0, , 89, AU, ES605, 845, M630, M660, X20,	bulleti	n		
Use After Free	21-11-2019	2.1	Use and daem static freed in Snape Snape Snape Snape Mobil Music Wears APQ8 APQ8 MDM MDM MDM	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905,				//ww lcom n/com produ ty/bu /octo 019- n	H-QUA- MDM9- 031219	/851
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8937, MSM8940, MSM8953, MSM896AU, MSM8953, MSM896AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/852
Buffer Copy without Checking Size of Input ('Classic	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in	https://ww w.qualcom m.com/com pany/produ ct-	H-QUA- MDM9- 031219/853
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	security/bu lletins/octo ber-2019- bulletin	
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/854

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2266		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150  CVE ID: CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MDM9- 031219/855
			Buffer over read can happen		
Out-of- bounds Read	21-11-2019	10	while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/856

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> SDM <sup>o</sup> SDA <sup>o</sup> SDM <sup>o</sup> SD	dragon_F 1130, SX						
Improper Authenticati on	21-11-2019	10	allow NAS result bypas Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM	CVE ID: CVE-2019-2271  Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,				//ww .com ./com produ ty/bu /octo 119- n	H-QUA- MDM9- 031219	/857
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description & CVE ID			Pat	ch	NCIIP	C ID
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130							
Integer Underflow (Wrap or Wraparound	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8064, IPQ8074, IPQ4019, IPQ8064, IPQ8074,			https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA- MDM9- 031219/858		
CV Scoring Scal (CVSS)	e 0-1	1-2	MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605,							

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297		
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM650, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MDM9- 031219/859

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID	
			CVE I	D : CVE-	2019-2	303					
N/A	21-11-2019	7.2	copy to the Parar are fr envir Auto, Snape Snape Snape Snape Snape Infras Netw APQ8 APQ8 APQ8 MDM MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8	e invoking from fd of secure leneters be om non somment. Snapdradragon Caragon Indragon Varagon Varagon, MS 19205, MS 1937, MS 1953, SD 1953,	or local labuffer, eing popsecure in Snapelagon Corsonsume adustria Mobile, Vired e and a APQ80 Q8053, Q8096A Q8053, Q8096A Q8053, Q8096A Q8053, QM9150, GM8920, GM8920, GM8920, GM8940, GM8940, GM8940, GM8940, GM8940, GM8940, GM8950, QM2645, SDM8940, GM8950, QM2645, SDM896, GM896, G	ouffer oulated dragon npute, vity, er IOT, l IOT, U, 09, U, 5, 09, W, 215, M429, M630, M660, M845, 17150, d_2016	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219		
mdm9607			TATE II			TATE TO A COLUMN TO THE TATE OF THE TATE O		https	/ /*****	H-QUA-	
Loop with Unreachable Exit	21-11-2019	5	Rejec	While processing Attach Reject message, Valid exit condition is not met			https:/ w.qual m.com	com	MDM9- 031219		
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch	NCIII	PC ID
Condition				ing into		ite loop	pany/p	orodu		
('Infinite				pdragor			ct-			
Loop')				lragon C			securit			
			•	lragon C			lletins			
			•	lragon Ir			ber-20			
			•	lragon Io	•	•	bulleti	n		
				e, Snapd	O	oice &				
				, Snapdr	_					
				ables in A	•	9,				
				017, AP(	•	_				
			·	096AU, A	•	•				
				9150, MI						
				9206, MI						
				9615, MI		•				
				9635M, I		•				
				9650, MI		•				
				3905, MS						
				3909W, I		•				
				3920, MS	•					
				3940, MS	•					
				8976, MS		AU,				
				3998, Nic		M045				
			-	150, QC						
				30X, SDA						
				29, SDM						
				30, SDM	•	•				
				60, SDM	•	•				
				45, SDM	•	•				
				5, SM615	•	150,				
				50, SM8		J 2016				
				lragon_H		a_2016				
			-	.130, SX						
			CVE I	D : CVE-	2019-2	335				
			Race	conditio	due to	the	https:/	/ww		
Time-of-			lack o	f resour	ce lock v	which	w.qual	com		
check Time-			will b	e concur	rently		m.com	/com	H-QUA-	-
of-use	21-11-2019	4.4	modif	ied in th	e memo	ру	pany/p	orodu	MDM9-	
(TOCTOU)			statement leads to out of						031219	
Race								y/bu		, = = =
Condition			Auto, Snapdragon Consumer l					octo/		
			Electr	onics Co	nnectiv	ity,	ber-20	19-		
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)				E/12						

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM' MDM' MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX2- SM81		ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8936, cobar, S405, Q0 60, SDA 1439, SD 1636, SD	l IOT, dragon dragon droice & 19, 19, 19, 19, 19, 19, 19, 19, 19, 19,	bulleti	n		
Use After Free	21-11-2019	2.1	daem static freed in Sna Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905,				//ww lcom l/com produ ty/bu /octo 019- n	H-QUA- MDM9- 031219	/863
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM896AU, MSM898, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/864
Buffer Copy without Checking Size of Input	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater	https://ww w.qualcom m.com/com pany/produ	H-QUA- MDM9- 031219/865
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	ct- security/bu lletins/octo ber-2019- bulletin	
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/866

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SM8150 CVE ID : CVE-2019-2266		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150  CVE ID: CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MDM9- 031219/867
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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, APQ8096AU, APQ8098,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/868
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	lragon_F I 130, SX	DM9607 DM9625 MDM9655 SM8909, MSM891 SM8940, SM8940, SM8940, SM8940, SM8956, MSM89 2150, Qu 1660, SD	98, CS605, M439, M632, M670, M850, ,				
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	/869
CV Scoring Scal	e 0-1	1-2	2-3	9615, MI	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	1	Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			MDM MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	9635M, I 9650, MI 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3996AU, bar, QCM 55, SC818 45, SDM 45, SDM 45, SDM 45, SDM 50, SDM 50, SM7 50, SM7 1130, SXI	DM9655 SM8909 MSM8937 SM8940 SM8976 MSM89 2150, Q 80X, SD 429, SD 1630, SD 1845, SD 1845, SD 150, SM	5, 17, , , , , , , , , , , , , , , , , ,				
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer while stand user's Auto, Electric Snape Snape Snape Infras Network APQ8 APQ8 IPQ40 MDM MDM MDM MSM8	r overflo processi ard NAN space. in Snapdra conics Co dragon I dragon M dragon W dragon W dragon W dragon W dragon W dragon W 17, APO 019, IPQS 9206, MI 9607, MI 9650, MS 3996AU, 574AU, O	w can o ing non messag Snapdra igon Con onsume ndustria Mobile, foice & M Vired and a APQ80 Q8053, Q8096A B064, IP DM9640 SM8905 QCA61	ccur ge from agon nsumer ity, er IOT, d IOT, U, Q8074, CQ8074,	https:/ w.qual m.com pany/i ct- securing lletins ber-20 bulleti	ty/bu /octo	H-QUA- MDM9- 031219	/870
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID: CVE-2019-2297		
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8909, MSM8909W, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM670, SDM710, SDM630, SDM670, SDM710, SDM750, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MDM9- 031219/871

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			, SXR2	1130, SX	R2130					
			CVE I	D : CVE-	2019-2	303				
N/A	21-11-2019	7.2	copy to the Paramare frenviro Auto, Snapo	invoking from fd of secure in the secure in	or local louffer, eing popsecure in Snapagon Coronsume adustria dobile, voice & March 1980, 1980	ouffer oulated dragon inpute, vity, in IOT, IOT, IOT, IOT, IOT, IOT, IOT, IOT,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219,	/872
msm8909w										
Loop with Unreachable	21-11-2019	5	While processing Attach Reject message, Valid exit			https:/ w.qual	•	H-QUA- MSM8-		
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	I	Descriptio	n & CVE	ID	Pat	ch	NCIIF	C ID
Exit			condi	tion is no	ot met		m.com	/com	031219	/873
Condition			result	ing into	an infini	ite loop	pany/j	orodu		
('Infinite			in Sna	pdragor	ı Auto,		ct-			
Loop')			•	lragon C	•		securit			
			•	lragon C			lletins			
			Snapo	lragon Ir	idustria	l IOT,	ber-20			
			•	lragon Ic	•	•	bulleti	n		
				e, Snapd	_	oice &				
				, Snapdr	•					
				ables in A	•	9,				
			•	017, APC	•					
				096AU, <i>A</i>	•					
				9150, MI		•				
				9206, MI		•				
				9615, MI		•				
				9635M, N		•				
				9650, MI						
				3905, MS						
				8909W, N		•				
				3920, MS	•					
				3940, MS						
				8976, MS		AU,				
				150, OC		M21 F				
			-	150, QC: 30X, SDA	_					
				29, SDM	•	•				
				30, SDM	•	•				
				50, SDM 60, SDM	•	•				
				45, SDM	•	•				
				5, SM615	•	•				
				50, SM82	•	130,				
				lragon_H		d 2016				
				.130, SXI		u_2010				
			-	•						
				D : CVE-						
Time-of-				condition			https:/	•		
check Time-				f resour		vhich	w.qual		11 0114	
of-use	21 11 2010	1.1		e concur	-		m.com	•	H-QUA-	
(TOCTOU)	21-11-2019	4.4		e memc		pany/p ct-	orodu	MSM8-	/074	
Race			statement leads to out of						031219	/8/4
Condition			bound access in Snapdragon					y/bu		
			Auto, Snapdragon Consumer   1				lletins	/octo		
CV Scoring Scal	0	1-2								

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81		onsume ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM893 GM8996, cobar, S405, Q0 60, SDA (439, SD (636, SD (636, SD	er IOT, l IOT, dragon oice & 9, 8, 7C, 0, , 89, AU, ES605, 845, M630, M660, X20,	ber-20 bulleti			
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905,				https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	/com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/875
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					ch	NCIIF	PC ID
			MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM8 SM61 SM82	3909, MS 3917, MS 3937, MS 3940, MS 3998, Nic 60, SDA 660, SDM 345, SDX 50, SM7 50, SXR2	M8920, M8939, M8953, M8996, cobar, Q 845, SDM 670, SD 20, SDX 150, SM	AU, CS605, M450, M710, 24, 8150,				
Improper Validation of Array Index	21-11-2019	4.6	CVE ID: CVE-2019-10490  Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM896AU, MSM8953, MSM896AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503				https://w.qualm.com/pany/jct-securitylletins/ber-20	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub				https:/ w.qual m.com	com	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	Pat	ch	NCIIP	C ID	
			Snapo Snapo Snapo Mobil Music Wears Wired Netwo IPQ40 MDM0 MDM0 MSM8 QCA9	les powe dragon A dragon In dragon Io dragon Io e, Snapdr ables, Sn d Infrastr orking in 019, IPQ8 9206, MI 9607, MS 980, QCS 445, SDX2	uto, onsume ndustria oT, Snap ragon V agon apdrago ucture APQ80 3064, DM9207 SM8909 Vicobar, 5405, Q0	r IOT, l IOT, dragon oice & on and 53, CC,	pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo )19-		
			CVE I	D : CVE-	2019-2	266				
Out-of- bounds Read	21-11-2019	10	while session messar un-information of Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8	r over reparsing on manages if netended values on Alragon Caragon Interpretables in Alragon Interpretables in Alragon, Mil 19635	downlingement of tworks alues in uto, ompute onsume ndustria oT, Snapragon Vagon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9655 MB909, MSM891	nk OTA ends  r IOT, l IOT, dragon oice &  9,  8,  6,  7,  40,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- MSM8- 031219	/878
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX20 SM61 SM82 Snapo	3939, MS 3953, MS 3996AU, ar, QCM 5, SC818 45, SDM 36, SDM 10, SDM 50, SM7 50, SM7 1130, SX D: CVE-	SM8976, MSM89 2150, Q0 30X, SDA 429, SDI 630, SD 660, SD 845, SD 7, SDX55 150, SM	98, CS605, A660, M439, M632, M670, M850, ,				
Improper Authenticati on	21-11-2019	10	Lack of allow. NAS in result bypas Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integriss MODEN nessages into aut is of NAS dragon A dragon C dragon Ic d	ity check M to accombined to chentical in uto, ompute onsume dustrial oT, Snap ragon APQ800 Q8053, APQ809 DM9205 DM9625 DM9625 MDM9645 SM8909, MSM8916, SM8940, SM8940,	ept any can tion  r IOT, l IOT, dragon oice &  9,  8,  7,  40,	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- MSM8- 031219	/879
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			QM21 SDA8- SDM6 SDM7 SDX2- SM61 SM82 Snapo	ar, QCM; 5, SC818 45, SDM 50, SDM 10, SDM 10, SDX24 50, SM7 50, dragon_H 130, SX	30X, SDA 429, SDI 630, SD 660, SD 845, SD 7, SDX55 150, SM High_Me R2130	A660, M439, M632, M670, M850, , 8150,				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	P modulout side it receives age. it saperal ragon Caragon Iragon Iragon, APC 096AU, APC 096AU, APC 09635M, Iragon, MI 09650, MI 09650, MI 09639, MS 0939,	its bour es malfo in Snapo gon Cor onsume idustria oT, Snap ragon V agon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9645 SM8909, MSM891 SM8937, SM8940, SM8940, SM8976, MSM89 2150, Q0 BOX, SDA 429, SDA	ndary ormed dragon inpute, r IOT, dragon foice & 9, 8, 5, 7, 7, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/880
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID: CVE-2019-2303		
msm8996au					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MSM8- 031219/881

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130		
			CVE ID: CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, 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, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150  CVE ID: CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MSM8- 031219/882
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcom m.com/com pany/produ ct- security/bu	H-QUA- MSM8- 031219/883
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	Pat	ch	NCIIP	C ID	
			Snapo Snapo Snapo Snapo Mobil Musio Wears APQ8 APQ8 MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM8 SM61 SM82	lragon C dragon I dragon I dragon I dragon I e, Snapdr ables in A 017, APC 096AU, A 9150, MS 9207C, M 9650, MS 3909, MS 3917, MS 3937, MS 3940, MS 3996, MS 3996, MS 3998, Nic 60, SDA 660, SDA 660, SDA 550, SXR 50, SXR 50, SXR	onsume ndustria oT, Snap ragon V ragon APQ800 Q8053, APQ809 DM960 SM8905 SM8905 SM8939, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953,	er IOT, I IOT, I IOT, I dragon foice & 9, 8, 5, 77, , W, CS605, M450, M710, 24, 8150,	lletins, ber-20 bulleti	19-		
Improper Validation of Array Index	21-11-2019	4.6	occur to imparray Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM	f-bounds in came proper verification Snapdra conics Codragon Codragon Magon Williagon	ra drive alidation Snapdr gon Cor onsume ndustria Mobile, foice & M Vearable Q8017, Q8096A M9206, MDM960	r due n of agon sumer ity, r IOT, l IOT, fusic, es in U,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/884
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	CVSS		Description	on & CVE	ID	Pat	:ch	NCIIP	CID
				MSM8 MSM8 MSM8 QCN7 SDM6 SDX2	3909W, 1 3920, MS 3940, MS 3996AU, 605, SD 530, SDM 0	5M8937, 5M8953, MSM89 A660, SI 1636, SD	, 98, DM450, M660,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-	-11-2019	2.1	varial firmw bound functi throu Auto, Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 MSM8 QCA6 QCS4 SDM8	oper valiole receivare cand accession while gh loop Snapdradragon Chagon Chagon Maragon Maragon Woss, APO 1996 AU, 574	ved from lead to of in WLAI e iteration in Snapo agon Con consume consume donnective donsume donnective donsume donnective donsume donnective donsume donnective donsume donnective donsume dustria dobile, MSM89 QCN760 605, SDA 20	n out of N ng dragon mpute, er rity, er IOT, dl IOT, Music in U, 198, 1845,	https:/w.qualm.com pany/ct- securilletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- MSM8- 031219	
Out-of- bounds Read	21-	-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in				https:/ w.qual m.com pany/ct- securi lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	е	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24		
			CVE ID: CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MSM8- 031219/887
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MSM8- 031219/888
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150  CVE ID: CVE-2019-2268	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MSM8- 031219/889

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Out-of- bounds Read	21-11-2019	10	while session messar un-interest of the session messar of the session mess	cover reparsing on manages if new dended with the dended with	downlingement etwork stalues in uto, ompute onsume industria oT, Snapuragon Vagon APQ800 DM9625 DM9625 DM9625 DM9625 DM9635 GM8909, MSM8937, GM8940, GM8976, MSM8940, GM8976,	nk OTA sends  , or IOT, ol IOT, olaragon olice & olice	https://w.qualm.com/pany/jct-securitelletins/ber-20	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/890
Improper Authenticati	21-11-2019	10	allow	of integr s MODEI nessages	M to acc	ept any	https:/ w.qual m.com	com	H-QUA- MSM8-	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Descriptio	n & CVE	ID	Pat	ch	NCIIP	CID		
on			result	into aut	hentica	tion	pany/j	produ	031219	/891		
			bypas	s of NAS	in		ct-					
			Snapo	lragon A	uto,		securit	ty/bu				
			Snapo	lragon C	ompute	,	lletins	octo/				
			Snapo	lragon C	onsume	r IOT,	ber-20	19-				
			Snapo	lragon Ir	ıdustria	l IOT,	bulleti	n				
			^	lragon Io	•	O						
				e, Snapd	_	oice &						
				, Snapdr	•							
				ables in A	•	9,						
				017, APC	•	_						
				096AU, A	•							
				9150, MI		•						
				9206, MI		•						
				9615, MI								
				9635M, I		•						
				9650, MI								
				3905, MS								
				3909W, N		•						
				3920, MS 3939, MS	•							
				3953, MS 3953, MS	•							
				3996AU,	•							
				ar, QCM		•						
				.5, SC818								
			•	45, SDM		•						
				50, SDM	•	,						
				36, SDM	•	•						
				10, SDM	•	•						
				0, SDX24	•	•						
				50, SM7								
			SM82		,	,						
			Snapo	lragon_H	ligh_Me	d_2016						
			_	[130, SX]	_							
			CVE I	D : CVE-	2019-2	289						
Integer			Buffer	r overflo	w can o	ccur	https:/	//ww				
Underflow			while	processi	ing non-		w.qual	com	H-QUA-			
(Wrap or	21-11-2019	4.6	standard NAN message from				standard NAN message from   m.com/co			-	MSM8-	
Wraparound			user space. in Snapdragon				pany/j	produ	031219	/892		
)			Auto, Snapdragon Consumer				ct-			•		
-			Electronics Connectivity,				securit	ty/bu				
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Date	CVSS	ı	Descriptio	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo Snapo Infras Netwo APQ8 IPQ40 MDM9 MDM9 MDM9 MSM8 QCA6 QCA9 QCS40 SDA8 SDM8 SM81		ndustria Jobile, Joice & N Vired and APQ80 Q8053, Q8096A B064, IP DM9640 SM8905 QCA617 QCA937 N7605, SO5, SDA 636, SDA 20, SDX	l IOT,  Music,  09,  U, Q8074,  7C, ), , 74A, 7,  1660, M660, 24,	lletins ber-20 bulleti	19-		
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Music Weara APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM	D: CVE- P modul out side it receiv lessage. i Snapdra dragon C dragon Ir dragon Ic e, Snapdr s, Snapdr ables in A 017, APC 096AU, A 9150, MI 9206, MI 9635M, I 9635M, I 9635M, I 9635M, I 9635M, I	e may adits bountes malfolic support the consumer of the consu	ccess indary formed dragon inpute, for IOT, fol IOT, foliagon foice &  19, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/893
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	lragon_H 130, SX	5M8940, 5M8976, MSM89 2150, Qu 30X, SDA 429, SDI 630, SD 6660, SD 845, SD 5, SDX55 150, SM	98, CS605, A660, M439, M632, M670, M850, ,				
				D : CVE-						
N/A	21-11-2019	7.2	copy for the the Paramare from	invoking from fd of secure because of secure because of secure for secure from none secure of se	or local bouffer, eing popsecure in Snape onnectivonsume dustria lobile, oice & Maria APQ80 (28053, Q8096A) (2	ouffer oulated dragon npute, vity, r IOT, l IOT, dusic, U,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- MSM8- 031219	/894

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDA6 SDM4 SDM6 SDM6 SDM8 SM81 Snapo , SXR1	lragon_I 130, SX <b>D : CVE-</b>	345, SDN 1450, SD 1636, SD 1710, SD 150, SM High_Me R2130 <b>2019-2</b>	M429, M630, M660, M845, 7150, d_2016				
Out-of- bounds Read	21-11-2019	2.1	Trustimemore result Snapo Snap	ecure Kozone to cory read into DO dragon Adragon Interesting in the corking in th	do an ar which which we's in auto, donnecting donsume and white and a APQ80 Q8096, IPQ8074 QCA808 QC	bitrary vill vity, r IOT, l IOT, lusic, 17, 4, 4, 1439, d_2016	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/895
qca6574au										
Improper Restriction of Operations within the Bounds of a	21-11-2019	2.1	varial firmw bound functi	oper vali ole recei vare can d access on while gh loop	ved fron lead to o in WLAl e iteratin	n out of N ng	https://w.qualm.com pany/jct-securit	com /com produ	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch:	NCIIP	CID
Memory Buffer			Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 MSM8 QCA6 QCS40 SDM8	Snapdra dragon C dragon C dragon I dragon W dragon V 053, APC 098, MD 3996AU, 574AU, C 05, QCSC 45, SDX	onsume onnectiv onsume ndustria lobile, foice & M Q8096A M9640, MSM89 QCN760 605, SDA	er ity, er IOT, l IOT, Music in U, 98,	lletins ber-20 bulleti	19-		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	wlan rates element than rates shaped Snaped Snaped Snaped Snaped Snaped APQ8 APQ8 MDM MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	r overflomodule in or extendent length max rate dragon Adragon Chagon Indragon Voltagon Volta	if suppo ded rate h is grea set leng uto, ompute onsume onsume onsume dustria Mobile, foice & M Q8053, MDM92 MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0 670, SDI 20, SM6	rted es ater gth in , er ity, er IOT, l IOT, Music in 06, 07, , CS605, M710, 150, R2130	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
Out-of-	21-11-2019	7.5	Possible OOB read issue in			https:/	//ww	H-QUA-	QCA6-	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	l	Descriptio	on & CVE	ID	Pat	ch	NCIIP	C ID
bounds Read			handl mana Snapo Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 SDA6 SDM6	ction fra ing WLA gement f dragon A dragon C dragon C dragon In dragon M dragon W 009, APC 053, APC 098, MD 9207C, M 9650, MS 379, QCS 60, SDM 660, SDM 645, SDX	frame in auto, consume on sume	or ity, or IOT, I IOT, Music in U, AU, A, 7, CS605, M636, M710, 150	w.qual m.com pany/j ct- securit lletins ber-20 bulleti	/com produ ty/bu /octo 119-	031219	/898
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electric Snape Snape Snape Snape Infras Network APQ8 APQ8 IPQ40 MDM MDM	r overflooprocessive NAN space. in Snapdra conics Codragon Indragon Varagon Varagon, APO 19, IPQ8 9206, MI 9607, MI 9607, MI 9650, MS	ing non- I messag Snapdra Igon Cor Innectiv Ionsume Industria Mobile, Vired In APQ80 Q8053, Q8096A B064, IP DM9640	ge from agon isumer ity, or IOT, lot, U, Q8074, 7C,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	_
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150		
			CVE ID : CVE-2019-2297		
qcs405					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150  CVE ID: CVE-2019-10486	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCS4- 031219/900

CV Scoring Scale	0-1	1_2	2-2	2-1	4-5	5-6	6-7	7₋0	8-0	0_10
(CVSS)	0-1	1-2	2-3	3-4	4-5	3-0	0-7	7-8	6-9	3-10

Weakness	Publish Date	CVSS	C	Description	n & CVE	ID	Pat	ch:	NCIIP	C ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	variab firmw bound function throug Auto, S Snapd Electry Snapd Snapd Snapd APQ80 APQ80 MSM8 QCA65 QCS40 SDM8	per valide receivance can laccess on while shapdra ragon Conics Conagon Irragon Vosa, APCO98, MDCO98,	ved from lead to of in WLAI e iteration in Snapo gon Cor onsume onsume onsume dustria dobile, oice & M 28096A MSM89 QCN760 05, SDA	n out of N ng dragon mpute, er rity, er IOT, dl IOT, U, 198, 195, 1845,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	_
Out-of- bounds Read	21-11-2019	4.6	in fast to imp while from f Snapd Snapd Snapd Snapd Snapd APQ80 MSM8 QCN70 SDA66 SDX20	messag proper in processi irmward ragon A ragon C ragon In ragon M ragon W 1953, APC 1996AU, 605, QCS 60, SDM 0, SDX24	e handle ing a me e in uto, onsume onsume onsume dustria lobile, oice & M 28096A MSM89 5405, Q0	er due idation essage er eity, er IOT, d IOT, Music in U, 198, CS605, M660,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- 031219	_
Buffer Copy without	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported				https:/ w.qual	•	H-QUA- 031219	_
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Checking Size of Input ('Classic Buffer Overflow')			elementhan respectively. Snapole Snapole Snapole Snapole Snapole Snapole APQ8 MDM MDM MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	or extendent length max rate dragon A dragon C dragon C dragon In dragon I dragon V 017, APC 096AU, I 9207C, M 9650, MS 3996AU, 174A, QC 45, SDM 45, SDM 50, SMS	h is greated set lenguto, ompute onsume onnectivonsume ondustriated bile, foice & March 1986 March 1986 March 1987 March	nter gth in  , er ity, er IOT, el IOT, Music in  06, 07, , CS605, M710, 150, R2130	m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from a source that the potent buffer Snape Snape Snape Snape Snape Snape Snape Snape APQ8	tmap file any un-a e, there i he bitma tially can dragon A dragon C	uthenticus a possible can use stack w. in uto, ompute onnectivonsume onsume dustrial lobile, foice & MQ8096A M9205,	cated sibility k  k  vity, er ity, er IOT, l	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Use After Free	21-11-2019	4.6	Nicob SA61: SDA8 SDM8 SM61 SM82 CVE I Possil kerne camer modu Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wear: Wired Netwo IPQ40 MDM MSM8 QCA9	ar, QCS4 55P, SC8 45, SDM 45, SDM 45, SDM 50, SXR D: CVE- ole doub I while he a senso les powellragon Id dragon Id d	1805, QCS 180X, S 1670, SD 1850, SD 150, SM 1130, SX 2019-2  le free is nandling r and its er seque ndustria oT, Snap dragon V ragon napdrago ructure n APQ80 8064, DM9207 SM8909 Nicobar, S405, Q0	605, DA660, M636, M710, X24, 8150, R2130  251  ssue in the sub ence in r IOT, l IOT, dragon oice & on and 53, 7C,	https:/w.qualm.company/jct-securitelletins/ber-20	//ww .com ./com produ ty/bu /octo	H-QUA- 031219	QCS4-
			CVE I	D : CVE-	2019-2	266				
Out-of- bounds Read	21-11-2019	7.5	P2P a handl mana Snapo Snapo Electr Snapo Snapo Snapo	ole OOB ction fra ing WLA gement dragon A dragon C dragon I dragon I dragon N	ames wh AN frame in Auto, Consume Consume Ionsume Mobile,	r ity, r IOT, l IOT,	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150  CVE ID: CVE-2019-2268		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM898, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCS4- 031219/907

Weakness	Publish Date	cvss	Description & CVE ID			Pat	ch	NCIIPC ID		
			CVE ID : CVE-2019-2295							
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electric Snape Snape Snape Infras Network APQ8 APQ8 IPQ40 MDM MDM MDM MSM8 QCA6 QCA9 QCS40 SDA8 SDM8 SM81	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297			https:/w.qualm.com pany/jct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-QCS4- 031219/908	
qcs605										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon			https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin		H-QUA-QCS6- 031219/909		
CV Scoring Scale (CVSS) 0-1		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo , SXR1	ables in A 017, APO 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MS 3905, MS 3905, MS 3976, MS 3976, MS 3976, MS 3976, MS 3976, SDA 429, SDM 530, SDM 545, SDM 545, SDM 545, SDM 545, SM615 1130, SX	Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 SM8909, MSM8937, SM8953, SM8953, SM8953, SM8953, SM8975, S605, Q1 1632, SD 1632, SD 1670, SD	8, 5, 7, 6, 40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM896AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150  CVE ID: CVE-2019-10486	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCS6- 031219/911
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo	H-QUA-QCS6- 031219/912
CV Scoring Scale (CVSS)	e 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM8	lragon C dragon In dragon Id e, Snapdr ables in A 017, APC 096AU, A 9150, MS 9207C, M 9650, MS 3909, MS 3917, MS 3940, MS 3996, MS 3996, MS 3996, MS 3996, MS 3996, MS 3996, MS 3996, MS 3996, SDAS 50, SDAS 50, SMAS	ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9206 MB905 SM8905 SM8939, SM89	l IOT, dragon dragon foice & 9, 8, 5, 77, W, CS605, M450, M710, 24, 8150,	ber-20 bulleti			
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	varial firmw bound functi throu Auto, Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 MSM8 QCA6	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845,				//ww com /com produ ty/bu /octo 119- n	H-QUA- 031219	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20		
			CVE ID : CVE-2019-10535		
Out-of- bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24  CVE ID: CVE-2019-10563	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCS6- 031219/914
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCS6- 031219/915
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	D	n & CVE	ID	Pat	ch	NCIIF	PC ID	
			QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130							
			CVE ID	: CVE-2	2019-1	0566				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from an source that the potential buffer of Snapdr	map file ny un-a , there i e bitma ially cau overflow ragon Co ragon Co ragon Co ragon Co ragon In ragon M ragon W 16, APC 198, MD 198, MD 15, SDM 15, SDM 16, SDM 16, SXR1 10, SXR1 10: CVE-2	uthentics a possip can use stack w. in uto, ompute onnectivonsume idustria lobile, oice & Marco	cated sibility k  k  vity, er ity, er IOT, al IOT, dusic in U, 10000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, 1000, 10	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &				w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	_
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
			Wears Wired Netwood IPQ40 MDM MDM MSM8 QCA9 SDM8 SM81		apdrago ructure a APQ80 3064, DM9207 SM8909 Nicobar, S405, Q0	and 53, 7C, , CS605, 150,				
Out-of- bounds Read	21-11-2019	7.5	CVE ID: CVE-2019-2266  Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150				https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in				https://w.qual m.com pany/j	com /com	H-QUA- 031219	•
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID					ch	NCIIF	PC ID
			Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musio Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	dragon A dragon C dragon I dragon I dragon I dragon I dragon I e, Snapdr ables in A 017, APC 096AU, A 9635M, I 9635M, I 9635M, I 9635M, I 9635M, I 3905, MS 3905, SDM 45, SDM 45, SDM 450, SDM 450, SDM 450, SDM 450, SDM 450, SM7 450, SM7 450, SM7 450, SM7 450, SM7 450, SM7 450, SM7 450, SM7	auto, ompute, onsume dustria oT, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9605 SM8909, MSM891 SM8937, SM8940, SM8976, MSM8976, MSM89 2150, Q0 30X, SDA 429, SDI 660, SD	r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, 40, 6, M439, M632, M670, M850, 8150, d_2016	securit lletins ber-20 bulleti	ty/bu /octo 119-		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,				https://w.qualm.com pany/jct- securit lletins/ber-20	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Snapo Snapo Mobil Music Wears APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	dragon Indragon Indragon Idragon Idrag	ndustria oT, Snap ragon V ragon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9645 DM9655 SM8909, MSM8916, MSM8976, MSM8976, MSM8940, SM8940, SM8940, SM8955, GM8976, MSM8955, MSM8976	l IOT, dragon foice & 9, 8, 5, 40, 5, 40, 5, M439, M632, M670, M850, 5,	bulleti			
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snapo Snapo Snapo Snapo Snapo Snapo	nation d k of addi done on dragon A dragon C dragon C dragon I dragon M	ress rang the Sys code. in outo, ompute onnectiv onsume adustria lobile,	ge DBG , vity, r IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description & CVE ID				ch	NCIIP	C ID
			Infras Netw APQ8 MDM MSM8 MSM8 MSM8 QCS4 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6	dragon_I 1130	e and n APQ80 Q8053, SM8905 SM8937, SM8937, SM8953, cobar, Q S05, QM: B450, SD I450, SD I710, SD	, CS404, 215, M429, M630, M660, M845,				
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer while stand user's Auto, Electric Snape Snape Snape Snape Infras Netw APQ8 APQ8 IPQ40 MDM MDM MDM MDM MSM8 QCA6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8064, IPQ8064, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605,				//ww lcom l/com produ ty/bu /octo 019- n	H-QUA- 031219	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSS	SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297  SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	Patch	NCIIPC ID
Out-of- bounds Read	21-11-2019	7.5	Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCS6- 031219/923

3-4

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	Description & CVE ID				Pat	ch	NCIII	PCID
N/A	21-11-2019	7.2	copy f to the Param are from environ Auto, s Snapd Snapd Snapd Snapd Snapd Infras Netwo APQ80 APQ80 APQ80 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SM81 Snapd SDM8 SNAPO SDM8 SNAPO SDM8 SNAPO SDM8 SNAPO SDM8 SNAPO SDM8 SNAPO SDM8 SNAPO SDM8 SNAPO SDM8 SNAPO SDM8 SDM8 SDM8 SDM8 SDM8 SDM8 SDM8 SDM8	invoking secure has ecure has en non soment. Snapdra lragon Calragon Iragon Waragon Waragon, MD 19607, MD 19607, MD 19607, MS 19607, SDM	or local bouffer, eing pope secure in Snape gon Corronsume dustria lobile, oice & Maried and APQ80 (28053, Q8096A) (28053, Q8053, Q8053, Q8054, Q8	ouffer oulated dragon inpute, vity, or IOT, l IOT,	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	_
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon				https:/ w.qual m.com pany/j ct- securit	com /com produ	H-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID: CVE-2019-2329	lletins/octo ber-2019- bulletin	
sda660					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDA6- 031219/926

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID			
			SDM8 SDX5 SM81 Snapo	660, SDM 45, SDM 5, SM61! 50, SM8 dragon_F 1130, SX <b>D : CVE-</b>	1850, SD 50, SM7 250, High_Me R2130	X20, 150, d_2016							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race of lack of will be modificated for the state of bound and the state of the sta	condition of resour e concur fied in the ment lead d access Snapdra conics Co dragon In dragon In dragon In dragon In dragon In e, Snapdra bles in 017, APO 096AU, A 9206, M 9650, M	n due to ce lock we rently e memo ds to out in Snapo in Snapo onsume dustria oT, Snapo dragon V ragon APQ809 DM9207 DM9207 DM9640 SM8905 MSM893 SM8996 cobar, S405, Q0 60, SDA (439, SD (636, SD (636, SD	the which rpy t of dragon rity, er IOT, dragon roice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-: 031219				
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting				daemon shutdown due to			https:/ w.qual m.com	com	H-QUA-	
CV Scoring Scale (CVSS)	e 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6				6-7	7-8	8-9	9-10			

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			freed in Snape Mobil Music Wears APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SM61 SM82	from a napdragon Calragon Calragon Calragon Indragon Indr	nultiple n Auto, compute connective consume ndustria oT, Snap dragon V ragon APQ800 APQ809 CMB920 CMB920 CMB939 CM	places  , vity, er IOT, el IOT, odragon oice &  9,  8, 6, 77, W, , AU, CS605, M450, M710, 24, 8150,	pany/j ct- securit lletins, ber-20 bulleti	produ ty/bu /octo 119-		
Improper Validation of Array Index	21-11-2019	4.6	occur to imp array Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8	f-bounds in came proper v index in Snapdra conics Co dragon In dragon V dragon V 009, APO 098, MD	ra drive alidation Snapdr Igon Con Igonective Igonectiv	er due n of cagon nsumer city, er IOT, al IOT, Music, es in U,	https:/ w.qual m.com pany/j ct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
				MDM MSM8 MSM8 MSM8 MSM8 QCN7 SDM6 SDX2	9207C, M 9640, M 3905, MS 3909W, M 3920, MS 3940, MS 605, SD 630, SDM 0	DM9650 5M8909, MSM8937, 5M8953, MSM89 A660, SI	), , , , , 98, OM450, oM660,				
Out-of- bounds Read	21-	-11-2019	4.6	in fasto important in fasto important in fasto important in from Snaportant in fasto important in fasto impo	r over-ret messag proper in process firmwar dragon A dragon I dragon I dragon I dragon V 053, APO 8996AU, 605, QC 60, SDM 0, SDX24	ge handlenput valing a mediuto, donsume onnective donsume ondustria Mobile, Moice & Mosma	er due idation essage er eity, er IOT, d IOT, Music in U, 198, CS605, M660,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-	-11-2019	7.2	from source that to potent buffer Snape Snape Snape Snape	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,				//ww lcom produ ty/bu /octo 019-	H-QUA- 031219	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3 3-4 4-5 5-6 6-7 7-8 8-9					8-9	9-10	

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIF	CID
			Snapo Snapo Snapo APQ8 APQ8 MSM8 Nicob SA61! SDA8 SDM6 SDM8 SM61 SM82	dragon C dragon I dragon V 016, APO 098, MD 3996AU, ar, QCS4 55P, SC8 45, SDM 660, SDM 50, SM7 50, SXR2	ndustria lobile, oice & M 28096A M9205, MSM89 05, QCS 180X, S 630, SD 670, SD 1850, SM	Music in U, 98, 6605, DA660, M636, M710, X24, 8150, KR2130				
Out-of- bounds Read	21-11-2019	7.5	Possil P2P a handl mana Snapo Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 SDA6 SDM8	ole OOB ction fra ing WLA gement f dragon A dragon C dragon C dragon I dragon M dragon W 009, APO 053, APO 098, MD 9207C, M 9650, MS 3998, QC 574AU, O 379, QC 60, SDM 660, SDM 660, SDM	read iss mes wh frame in uto, onsume onsume dustria lobile, oice & M 28017, 28096A M9206, MDM960 SM8996 A6174A QCA937 S405, QO 630, SD 6670, SD	ue in ile  er erity, er IOT, el IOT, Music in  U, 7, AU, A, 77, CS605, M636, M710, 150	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Out-of- bounds Read	21-11-2019	10		r over re parsing			https:/ w.qual	•	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIII	PC ID
	Publish Date	CVSS	session messa un-introduced snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musico Wears APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	on manage ages if new tended voltagon Adragon Coltagon Indragon In	gement (etwork stalues in uto, ompute, onsume dustria of, Snap ragon Vagon APQ800 DM9605 DM96	oTA sends  r IOT, l IOT, dragon oice &  9, 8, 5, 40, 5, 47, 47, 48, 68, 69, 4850, 4850, 4850, 69, 8150, 60, 60, 60, 60, 60, 60, 60, 60, 60, 6	m.com pany/j ct- securit lletins, ber-20 bulleti	//ww		
Improper Authenticati on	21-11-2019	10	allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in  w.qualco m.com/c pany/pro ct-						H-QUA-031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musio Wears APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	dragon Adragon Colragon Colragon Indicated In Italian Indicated In Itali	uto, ompute, onsume dustria oT, Snap ragon APQ800 Q8053, APQ809; DM9625 DM9625 MDM9625 MSM8909, MSM8916, MSM8976, MSM897	r IOT, l IOT, dragon oice & 9, 8, 40, 5, 40, 5, 40, 5, 40, 6, 40, 6, 40, 6, 8150, M632, M670, M850, 9, 8150,	securit lletins ber-20 bulleti	ty/bu /octo 119-		
Improper Restriction of	21-11-2019	2.1	Inform to lack check	nation d k of addr done on	isclosur ess rang the Sys	e due ge DBG	https:/ w.qual m.com pany/j	com /com	H-QUA-	SDA6-
Operations within the Bounds of a Memory	21-11-2019	2.1	Snapo Snapo Snapo	lragon A lragon C lragon C lragon C	uto, ompute, onnectiv	, vity,	ct- securit lletins, ber-20	ty/bu /octo	031219	/935
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	ch	NCIIP	C ID
Buffer			Snapo Snapo Snapo Infras Netwo APQ8 MDM' MSM8 MSM8 MSM8 QCS40 SDA6 SDM6 SDM6 SDM6 SDM6 SDM8	dragon_H	Mobile, Moice & Movired Mand Mand APQ80 Mand	Music,  009,  CS404,  215,  M429,  M630,  M660,  M845,  d_2016	bulleti	n		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electr Snapo Snapo Snapo Infras Netwo APQ8 APQ8 IPQ40 MDM MDM MDM MDM	r overflo processi ard NAN space. in Snapdra conics Co dragon C dragon M dragon W dragon W dragon W dragon W dragon W 19, IPQ8 9607, MI 9607, MI 9650, MS	ing non- imessage Snapdra igon Cor onnectiv onsume idustria fobile, foice & M Vired and APQ80 Q8053, Q8096A B064, IP DM9207 DM9640	ge from agon isumer ity, er IOT, l IOT, Music, Q8074, 7C, ),	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			QCA9 QCS46 SDA8 SDM8 SM81 CVE I	<b>D : CVE-</b> P modul	N7605, 05, SDA 636, SDI 20, SDX2 2019-2 e may ac	.660, M660, 24, <b>297</b> ccess				
Out-of- bounds Read	21-11-2019	7.5	when XID mand Auto, Snaped Snaped Snaped Snaped Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	out side it receive it ragon In it ragon, MI it ragon	res malfo in Snapo gon Corr onsume dustria oT, Snap ragon APQ800 Q8053, APQ809 OM9607 OM9607 OM9607 OM9655 MB909, MSM891 SM8937, SM8940, SM8940, SM8940, SM8940, SM8940, SM8940, SM8940, SM8956, MSM89 2150, Q0 30X, SDA 429, SDA 429, SDA 630, SDA 630, SDA 5, SDX55 150, SM	ormed dragon inpute, r IOT, dragon foice & 9, 8, 5, 7, 6, 40, 6, 7, 40, 6, 4660, M439, M632, M670, M850, 6, 8150, 8	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-: 031219	
CV Scoring Scal	e 0.4	1.3					6.7	7.0	0.0	0.40
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			, SXR1	1130, SX	R2130					
			CVE I	D : CVE-	2019-2	303				
N/A	21-11-2019	7.2	copy for the Paramare from the	e invoking from fd of secure is neters be om non soment. Snapdradragon Chagon Indragon Williagon Williagon, Milliagon, SDM 630, SDM 630, SDM 630, SDM 630, SDM 630, SM 6	or local lands of loc	ouffer oulated dragon inpute, vity, er IOT, l IOT,	https://w.qualm.company/jct-securitelitins/ber-20bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
sdm439										
Loop with Unreachable	21-11-2019	5		process t messag	•		https:/ w.qual	•	H-QUA-	SDM4-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIII	PC ID
Exit			condi	tion is no	ot met		m.com	/com	031219	9/939
Condition				ing into		ite loop	pany/j	orodu		
('Infinite			in Sna	ıpdragor	ı Auto,		ct-			
Loop')			•	lragon C	•		securit			
			•	lragon C			lletins			
			Snapo	lragon Ir	ıdustria	l IOT,	ber-20	19-		
			•	lragon Io	•	O	bulleti	n		
				e, Snapd	_	oice &				
				, Snapdr	•					
				ables in A	•	9,				
				017, APC	•					
				096AU, <i>I</i>	•					
				9150, MI		•				
				9206, MI		•				
				9615, MI		•				
				9635M, I		•				
				9650, MI						
				3905, MS						
				3909W, N		•				
				3920, MS	•					
				3940, MS						
				3976, MS		AU,				
				3998, Nic		M215				
			_	2150, QC	_					
				30X, SDA	•	•				
				29, SDM	•	•				
				30, SDM	•	•				
				60, SDM	•	•				
				45, SDM	•	•				
				5, SM615	•	150,				
				50, SM82		J 2017				
				lragon_H l 130, SXI		u_2016				
			-	•						
			CVE I	D : CVE-	2019-2	335				
Time-of-				conditio			https:/	•		
check Time-			lack o	f resour	ce lock v	which	w.qual	com		
of-use			will be concurrently m.com/c			/com	H-QUA-	SDM4-		
(TOCTOU)	21-11-2019	4.4	modified in the memcpy pany/produ 031219/9							
Race		statement leads to out of ct-							,	
Condition		bound access in Snapdragon security/bu								
		Auto, Snapdragon Consumer   lletins/octo								
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)				508						

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo Snapo Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81	ronics Colragon C dragon Indragon Ide e, Snapdr de, Snapdr debles in A 017, APC 096AU, A 9607, MI 9650, MS 3909W, I 3953, MS 3998, Nic 605, QCS 5, SDA6 29, SDM 10, SDM 10, SDM 10, SDM 10, SDM	onsumendustria oT, Snap ragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM893 cobar, S405, Q0 60, SDA (439, SD (636, SD (845, SD	r IOT, l IOT, dragon oice & 9, 8, 7C, 9, AU, S605, 845, M630, M660, X20,	ber-20 bulleti	-		
Out-of- bounds Read	21-11-2019	10	while session messar un-interpretation of the session messar un-interpretation of the session of	r over reparsing an manage of the decident of	downlingement (etwork straines in uto, ompute, onsume ndustria oT, Snap ragon Vagon APQ800 Q8053, APQ809 DM9607	nk OTA ends  r IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	dragon_F 1130, SX	DM9655 M8909, MSM891 SM8937, SM8976, MSM89 2150, Q0 30X, SDA 429, SDA 660, SD 660, SD 845, SD 7, SDX55 150, SM	98, CS605, A660, M439, M670, M850, ,				
				D : CVE-						
Improper Authenticati on	21-11-2019	10	allow NAS r result bypas Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MDM	of integrals MODEI messages into aut ss of NAS dragon A dragon C dragon I dragon I dragon I dragon I dragon I ge, Snapdr ables in A 9150, MI 9206, MI 9635M, I 9635M, I 9635M, I 9635, MS	M to accombined to accombine the second to accombine t	ept any can tion  r IOT, l IOT, dragon oice & 9, 8, 5, 7, 7, 7, 140, 15, 15, 15, 15, 15, 15, 15, 15, 15, 15	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

MSM8909W, MSM8917, MSM8937, MSM8930, MSM8937, MSM8939, MSM8936, MSM8936, MSM8936, MSM8936, MSM8936, MSM8936, MSM8936, MSM8996, MSM8996, MSM8996, MSM8996, MSM8996, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDM630, SDM632, SDM636, SDM6450, SDM450, SDM450, SDM450, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX20, SDX24, SDX55, SM6150, SM7150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130    CVE ID : CVE-2019-2289	Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8905, MSM8907, MSM8920, MSM8937,  **To lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8905, MSM8905, MSM8907, MSM8909, MSM8917, MSM8920, MSM8937,				MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX2 SM61 SM82 Snapo	8920, MS 8939, MS 8953, MS 8996AU, par, QCM 15, SC818 45, SDM 450, SDM 710, SDM 710, SDM 50, SM7 850, dragon_H	5M8937, 5M8940, 5M8976, MSM89 2150, Q0 80X, SDA 429, SDI 1630, SD 1660, SD 1660, SD 1845, SD 150, SM High_Me R2130	98, CS605, A660, M439, M632, M670, M850, ,				
MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	Restriction of Operations within the Bounds of a Memory	21-11-2019	2.1	Information lack check buffer Snape	mation d k of addi c done or rs in SDI dragon A dragon O dragon I dragon W dragon W dragon W structure orking in 8920, MS 8920, MS 8940, MS 8940, MS	isclosur ress rang the Sys code. in auto, compute connective consume dobile, foice & M Vired and APQ80 Q8053, SM8905 SM8917, SM8937, SM8953, cobar, Q 605, QM2 605, SDM	e due ge DBG  vity, r IOT, l IOT, fusic,  CS404, 215, M429, M630,	w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	•	
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	_	e 0-1	1-2				6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295		
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM650, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4- 031219/944

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8953, MSM8996, MSM896AU, APQ8098, APQ8096AU, APQ8098, MSM8917, MSM8920, MSM8917, MSM8920, MSM8917, MSM8940, MSM8953, MSM8996, MSM896AU, MSM8996, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA645, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4- 031219/945
Out-of- bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in	https://ww w.qualcom m.com/com pany/produ	H-QUA-SDM4- 031219/946

3-4

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318	ct- security/bu lletins/octo ber-2019- bulletin	
sdm630					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6- 031219/947

3-4

4-5

6-7

7-8

8-9

9-10

5-6

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Dat	e CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	3909W, 1 3920, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDM 229, SDM 30, SDM 345, SDM 55, SM61: 50, SM8 dragon_H	5M8937, 5M8953, 5M8996, cobar, S605, Q 1632, SD 1632, SD 1670, SD 1850, SM7 250, High_Me	M215, AU, M215, A845, M450, M636, M710, X20,				
				D : CVE-						
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-201	9 4.4	lack of will be modified stater bound Auto, Electric Snape Mobil Music Wears APQ8 APQ8 MDM MDM MDM MSM8 MSM8 MSM8 QCN7	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845,				//ww lcom l/com produ ty/bu /octo 019- n	H-QUA- 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM7	32, SDM 10, SDM 4, SM61! 50	1845, SD	X20,				
			CVE I	D : CVE-	2019-1	0486				
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM896AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
				D : CVE-						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer			https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin		H-QUA- 031219		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130							
			P2P a handl mana Snapo Snapo Electr Snapo Snapo Snapo	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in			https:/ w.qual m.com	com /com		
Out-of- bounds Read	21-11-2019	7.5	APQ8 APQ8 MDM' MDM' MSM8 QCA6 QCA9 SDA6 SDM6	APQ8009, APQ8017, APQ8053, APQ8096AU,		ct- securit lletins ber-20 bulleti	ty/bu /octo )19-	H-QUA-		
Out-of-	21-11-2019	10	Buffer over read can happen			https:/	//ww	H-QUA-	SDM6-	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	I	Descriptio	n & CVE	ID	Pat	ch	NCIIF	PC ID
bounds Read			while	parsing	downlir	nk	w.qual	com	031219	/952
			sessio	n manag	gement	OTA	m.com	/com		
			messages if network sends				pany/j	orodu		
			un-int	tended v	alues in		ct-			
			•	lragon A	•		securit	y/bu		
				lragon C			lletins			
			•	lragon C		•	ber-20			
			_	lragon Ir			bulleti	n		
			^	lragon Io	•	•				
				e, Snapd	•	oice &				
				, Snapdr	•	_				
				ables in A	•	9,				
			-	017, APC	•	_				
			-	096AU, A	•					
				9150, MI						
				9206, MI		-				
				9615, MI						
				9635M, I		•				
				9650, MI		•				
				3905, MS	•					
				3909W, N		•				
				3920, MS						
				3939, MS 3953, MS						
				3933, M3 3996AU,						
				ar, QCM						
				.5, SC818		•				
			~	45, SDM	•	•				
				50, SDM	•	•				
				36, SDM	•	•				
				10, SDM	•	•				
				0, SDX24	•	•				
				50, SM71						
			SM82		100,014	0100,				
				lragon_H	ligh Me	d 2016				
				130, SXI		~_ <b>2</b> 010				
				<b>D</b> : <b>CVE</b> -		271				
Imamarata			Lack	of integri	ty checl	k	https:/	//ww		
Improper	21 11 2010	10	allows MODEM to accept any					com	H-QUA-	SDM6-
Authenticati	21-11-2019	10	NAS messages which can					/com	031219	/953
on			result into authentication					orodu		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	Pat	ch	NCIIF	PC ID	
			bypass of NAS in				ct-			
			Snapdragon Auto,				securi			
			•	lragon C	•		lletins			
			_	lragon C			ber-20			
			_	lragon Ir			bulleti	n		
			•	lragon Io		O				
				e, Snapd	•	oice &				
				, Snapdr	_	0				
				ables in A	•	9,				
			•	017, AP(	•	O				
			•	096AU, A	•					
				9150, MI 9206, MI						
				9615, MI		•				
				9635M, I		•				
				9650, MI		•				
				3905, MS						
				3909W, I	•					
				3920, MS						
				3939, MS	•					
				3953, MS						
				3996AU,						
			Nicob	ar, QCM	2150, Q	CS605,				
			QM21	.5, SC818	30X, SD <i>A</i>	A660,				
			SDA8	45, SDM	429, SDI	M439,				
			SDM4	50, SDM	630, SD	M632,				
			SDM6	36, SDM	660, SD	M670,				
			SDM7	10, SDM	845, SD	M850,				
			SDX2	0, SDX24	, SDX55	,				
			SM61	50, SM7	150, SM	8150,				
			SM82	•						
				lragon_F		d_2016				
			, SXR1	[130, SX]	R2130					
			CVE I	D : CVE-	2019-2	289				
Improper			Inform	nation d	isclosur	e due	https:/	//ww		
Restriction			to lac	k of addr	ess rang	ge	w.qual	com		
of			check	done on	the Sys	DBG	m.com	/com	H-QUA-	SDM6-
Operations	21-11-2019	2.1	buffer	rs in SDI	code. in		pany/	produ	031219	
within the			_	lragon A			ct-			,
Bounds of a				lragon C			securi			
Memory			Snapdragon Connectivity,				lletins	/octo		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Buffer			Snapo Snapo Snapo Infras Netwo APQ8 MDM <sup>o</sup> MSM8 MSM8 MSM8 QCS40 SDM6 SDM6 SDM6 SDM6 SDM8 Snapo , SXR1	lragon_H	ndustria Mobile, Moice & M Vired and APQ80 Q8053, SM8905 SM8937, SM8953, Cobar, Q M8953, Cobar, Q M8953, Cobar, Q M8953, Cobar, Q M8953,	l IOT, fusic, 09, , CS404, 215, M429, M630, M660, M845, d_2016	ber-20			
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX2 SM61 SM82 Snapo	dragon_H 1130, SXI	M8937, M8940, M8976, MSM89 2150, Q0 30X, SDA 429, SDI 630, SD 660, SD 845, SD 5, SDX55 150, SMS	98, CS605, A660, M439, M632, M670, M850, ,				
N/A	21-11-2019	7.2	While copy is to the Param are from the Param are f	e invoking from fd of secure is neters becoment. Snapdradragon Caragon Indragon Waragon Waragon, MD 9205, MD 9205, MD 9205, MS 937, MS 937, MS 937, MS 937, MS 937, MS	g the AP or local brouffer, eing popsecure in Snape gon Consume adustria lobile, oice & Maried and a APQ80 (8053, Q8096A) (M9150, QM9206 (M8909, EM8940, EM894	I to puffer ulated dragon npute, vity, r IOT, I IOT, I USIC,	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
sdm660					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM898, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM6- 031219/957

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch:	NCIIF	PC ID
			SDM6 SDM8 SDX5 SM81 Snapo , SXR1	30, SDM 60, SDM 45, SDM 5, SM61! 50, SM8 dragon_F 1130, SX <b>D : CVE</b> -	670, SD 850, SD 50, SM7 250, High_Me R2130 <b>2019-2</b>	M710, X20, 150, d_2016				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated to will be modifi	condition f resour f resour e concur fied in the nent lead d access Snapdra fonics Co dragon In dragon In dragon In dragon In e, Snapdra sbles in 1 017, APO 096AU, 1 9206, Mi 9650, Mi	ce lock werently e memorish so our in Snape in Snape in Gornective onsume industria oT, Snape ragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905	which  py t of dragon nsumer ity, or IOT, l IOT, dragon oice &  9,  8, 7C, 0, , 89, AU, CS605, 845, M630, M660, X20, 150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Use After	21-11-2019	2.1	Use after free issue in Xtra				https://ww		H-QUA-	SDM6-
Free		2.1	daem	on shutc	lown du	e to	w.qual	lcom	031219	/959
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			static freed in Snape Snape Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM	object ir from a napdragon Caragon Caragon Ir dragon Ir	astance and tiple and Auto, ompute, onnectivonsume and stria of T, Snap aragon Vagon APQ800 APQ809 A	getting places vity, r IOT, l IOT, dragon oice & 9, 8, 7, W, CS605, M710, 24, 8150,	m.com pany/j ct- securit lletins ber-20 bulleti	produ ty/bu /octo 119-		
Improper Validation of Array Index	21-11-2019	4.6	occur to imparray Auto, Electr Snapo Snapo Snapo Snapo Snapo APQ8	f-bounds in came proper veindex in Snapdra conics Codragon Codragon Miragon Wiragon Wiragon Wiragon Wiragon Wiragon Wiragon Wiragon Wiragon APO	ra drive alidation Snapdr gon Cor onsume ndustria Jobile, Joice & M Vearable Q8017,	r due n of agon isumer ity, r IOT, l IOT, fusic, es in	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	Pat	ch	NCIIP	C ID	
			MDM <sup>o</sup> MSM8 MSM8 MSM8 MSM8 QCN7 SDM6 SDX2	098, MD 9207C, M 9640, MS 8905, MS 8920, MS 8920, MS 8940, MS 8996AU, 605, SDM 0	MDM9650 DM9650 SM8909, MSM891 SM8953, MSM89 A660, SI	98, 0M450, M660,				
Out-of- bounds Read	21-11-2019	4.6	in fast to imp while from a Snapo Sn	r over-ret message proper in process firmwar dragon Adragon Coloragon Indragon Word, APO 18996AU, 605, QC 18	ge handle ing a me e in tuto, consume consume dobile, voice & M Q8096A MSM89 S405, Q0	er due idation essage r ity, r IOT, l IOT, l IOT, 98, CS605, M660,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	/com /com produ ty/bu /octo	H-QUA- 031219	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer				https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo APQ8 APQ8 MSM8 Nicob SA61! SDA8 SDM6 SDM8 SM61 SM82	ronics Co dragon C dragon M dragon V 016, APO 098, MD 3996AU, ar, QCS4 55P, SC8 45, SDM 660, SDM 50, SM7 50, SXR2	onsume ndustria lobile, loice & M Q8096A M9205, MSM89 405, QCS 180X, SI 1670, SD 1850, SD 150, SM	er IOT, d IOT, Music in U, 98, 6605, DA660, M636, M710, X24, 8150, (R2130				
			Possil P2P a	ole 00B ction fra	read iss mes wh	ue in				
Out-of- bounds Read	21-11-2019	7.5	mana Snapo Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 SDA6 SDM6	Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU,		https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219		
Out-of-	21-11-2019	10	Buffer	r over re	ad can h	nappen	https:/	//ww	H-QUA-	SDM6-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	I	Descriptio	n & CVE	ID	Pat	ch	NCIIF	PC ID
bounds Read			while	parsing	downlir	nk	w.qual	com	031219	/964
			sessio	n manag	gement	OTA	m.com	/com		
			messa	iges if ne	twork s	ends	pany/j	orodu		
			un-int	tended v	alues in		ct-			
			Snapo	lragon A	uto,		securit	y/bu		
			Snapo	lragon C	ompute	,	lletins	octo/		
			Snapo	lragon C	onsume	r IOT,	ber-20	19-		
			Snapo	lragon Ir	ıdustria	l IOT,	bulleti	n		
			Snapo	lragon Io	T, Snap	dragon				
			Mobil	e, Snapd	ragon V	oice &				
				, Snapdr	•					
			Weara	ables in A	APQ800	9,				
			APQ8	017, APO	)8053,					
			-	096AU, <i>I</i>	•					
			MDM	9150, MI	OM9205	, ,				
				9206, MI		-				
			MDM	9615, MI	DM9625	<b>,</b>				
			MDM	9635M, I	MDM96	40,				
				9650, MI		•				
				3905, MS	•					
				3909W, N		•				
				3920, MS						
				3939, MS						
				3953, MS						
				3996AU,						
				ar, QCM		•				
			~	5, SC818	•	•				
				45, SDM	•	•				
				50, SDM	•	•				
				36, SDM	•	•				
				10, SDM	•	•				
				0, SDX24						
				50, SM7	150, SM	8150,				
			SM82	•						
				lragon_H		d_2016				
			, SXR1	130, SX	R2130					
			CVE I	D : CVE-	2019-2	271				
Improper			Lack o	of integri	ty checl	k	https:/	//ww		
Authenticati	21-11-2019	10	allow	ept any	w.qual	com	H-QUA-	SDM6-		
on	21 11-2019	10	NAS messages which can					/com	031219	/965
OII			result	into aut	hentica	tion	pany/j	orodu		
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
			٠.	s of NAS			ct-			
			•	lragon A	•		securi			
			•	lragon C	•		lletins			
			_	lragon C			ber-20			
			•	lragon Ir		•	bulleti	n		
				lragon Io						
				e, Snapd	•	oice &				
				, Snapdr	-	0				
				ables in A	_	9,				
			•	017, APO 096AU, A	•	0				
			•	9150, MI	•					
				9130, MI 9206, MI						
				9615, MI		•				
				9635M, I						
				9650, MI		•				
				3905, MS						
				3909W, I	•					
				3920, MS		•				
				3939, MS	•					
				3953, MS						
				3996AU,						
			Nicob	ar, QCM	2150, Q0					
			QM21	.5, SC818	30X, SD <i>A</i>					
			SDA8	45, SDM	429, SDI	M439,				
			SDM4	50, SDM	630, SD	M632,				
			SDM6	36, SDM	660, SD	M670,				
			SDM7	10, SDM	845, SD	M850,				
			SDX2	0, SDX24	, SDX55	,				
			SM61	50, SM7	150, SM	3150,				
			SM82	•						
				lragon_F		d_2016				
			, SXR1	[130, SX]	R2130					
			CVE I	D : CVE-	2019-2	289				
Improper			Inform	nation d	isclosur	e due	https:/	//ww		
Restriction			to lac	k of addr	ess rang	ge	w.qual	com		
of			check	done on	the Sys	DBG	m.com	/com	H-QUA-	SDM6-
Operations	21-11-2019	2.1	buffer	rs in SDI	code. in		pany/	produ	031219	
within the			Snapdragon Auto,							,
Bounds of a			Snapdragon Compute,					ty/bu		
Memory			Snapo	lragon C	onnectiv	ity,	lletins	/octo		
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8909, MSM8917, MSM8990, MSM8953, MSM8998, MSM8993, MSM893, MSM8993, MSM893,	Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,  While processing non-standard NAN message from user space. in Snapdragon https://www.qualcom m.com/com pany/produ ct-security/bu lletins/octo ber-2019- bulletin  H-QUA-SDM6-031219/967	Buffer			Snapo Snapo Snapo Infras Netwo APQ8 MDM <sup>o</sup> MSM8 MSM8 MSM8 QCS40 SDM6 SDM6 SDM6 SDM6 SDM8 Snapo , SXR1	dragon Indragon Maragon Walragon Walragon Walragon Walragon, MS 3920, MS 3940, MS 3998, Nico 39, SDM 370, SDM 3	ndustria Mobile, Moice & M Vired and APQ80 Q8053, SM8905 SM8937, SM8953, Cobar, Q M345, SDM M450, SD M450, SD M1450, SD	CS404, 215, M630, M645, M2016				
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Underflow (Wrap or Wraparound	21-11-2019	4.6	while stand user's Auto, Electric Snape Sn	procession NAN space. in Snapdra conics Colragon Chagon Magon Waragon Waragon Waructure 17, APO 19, IPQ 19, IPQ 19, IPQ 19607, Mill 19607,	ing non- imessage Snapdra igon Cor onsume idustria Mobile, Toice & M Vired and APQ80 Q8053, Q8096A B064, IP DM9640	ge from agon asumer ity, r IOT, l IOT	w.qual m.com pany/i ct- securit lletins ber-20	com /com produ ty/bu /octo	•	
	_	e <b>0-1</b>	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			QCA6 QCA9 QCS4 SDA8 SDM8 SM81	D : CVE-	QCA937 N7605, 605, SDA 636, SD 20, SDX	7, 4660, M660, 24, <b>297</b>				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modulout side it receive lessage. Snapdradragon Idragon Idra	its bounces malformatical in Snapolagon Consumer industrial of The Snapolagon Veragon	ndary ormed dragon inpute, er IOT, il IOT, odragon voice & 19, 18, 5, 7, 17, 17, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18	https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA-3 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 <b>CVE ID : CVE-2019-2303</b>		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8953, MSM8996, SSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6- 031219/969
sdx20					

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pat	ch	NCIII	PC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condit resulti in Snap di SNAS SNAS SNAS SNAS SNAS SNAS SNAS SNA	process messag ion is no ng into pdragor ragon C ragon Ic ragon Ic snapdr bles in A 017, APC 096AU, A 0150, MI 0635M, I	re, Valid of met an infin in Auto, ompute onsume industria oT, Snap ragon Vagon APQ809 DM9607 DM9605 DM8905 DM895	exit ite loop , er IOT, l IOT, dragon foice &  9,  8, 5, 7, 6, 40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150, d_2016	https://w.qualm.company/jct-securitelletins/ber-20bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Time-of- check Time- of-use (TOCTOU) Race	21-11-2019	4.4	lack of will be modifi	ondition resource concur ed in th	ce lock v rently e memc	which	https:/ w.qual m.com pany/j	com /com	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
Condition			Auto, Electric Snaped Snaped Snaped Snaped Snaped Mobil Music Wears APQ8 MDM9 MDM9 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81 CVE III	D : CVE-	agon Coronnective Consume Industria oT, Snap Iragon Varagon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 SM8996 Cobar, S405, Q0660, SDA 1439, SDA 1439, SDA 1636, SDA 163	nsumer ity, er IOT, IOT, dragon foice & 9, 8, 7C, 9, AU, CS605, 845, M630, M660, X20, 150, 150, 150, 150, 150, 150, 150, 15	securit lletins ber-20 bulleti	octo 19-		
Use After Free	21-11-2019	2.1	daemo static freed in Sna Snapo Snapo Snapo Snapo Mobil Music Weara APQ8 APQ8	ter free on shutd object in from a napdragon Caragon Caragon Caragon Caragon Indicagon	down dunstance sometion Auto, Compute Consume oT, Snap dragon Vagon APQ800 Q8053, APQ809	e to getting places  vity, or IOT, l IOT, dragon foice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-9	
CV Scoring Scale			2-3 3-4 4-5 5-6						1	

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch:	NCIIP	C ID
			MDM <sup>o</sup> MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM8 SM61 SM82	9207C, M 9650, MS 3909, MS 3917, MS 3940, MS 3996, MS 3998, Nic 60, SDA8 660, SDA8 660, SDM 545, SDX 50, SXR2	5M8905 5M8909 5M8939, 5M8953, 5M8996, 5obar, Q 6670, SD 20, SDX 2130	, W, AU, CS605, M450, M710, 24, 8150,				
Improper Validation of Array Index	21-11-2019	4.6	occur to imparray Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDX20				//ww lcom produ ty/bu /octo 019- n	H-QUA- 031219	
Improper	21-11-2019	2.1	Improper validation for loop			https:/	//ww	H-QUA-	SDX2-	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	e CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
Restriction of Operations within the Bounds of a Memory Buffer			firmw bound functi throu Auto, Snapo Snapo Snapo Snapo APQ8 APQ8 MSM8 QCA6 QCS4 SDM8	ole receivare can d access on while gh loop is Snapdra dragon Conics Conics Conics Conics dragon Maragon Maragon Maragon Williagon Willi	lead to of in WLAI enteration Snaped gon Coreon Sume andustria Mobile,	out of N ng dragon npute, or ity, or IOT, I IOT, U, 98, 5,	w.qual m.com pany/j ct- securit lletins ber-20 bulleti	/com produ ty/bu /octo 119-	031219	/974
Out-of- bounds Read	21-11-201	9 4.6	CVE ID: CVE-2019-10535  Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24  CVE ID: CVE-2019-10563				https:/ w.qual m.com pany/j ct- securif lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-	
Buffer Copy without Checking	21-11-201	9 4.6	Buffer overflow can occur in wlan module if supported rates or extended rates				https:/ w.qual m.com	com	H-QUA-	
CV Scoring Scal (CVSS)	e 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Size of Input ('Classic Buffer Overflow')			than r Snapo Snapo Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	ent length max rate dragon A dragon C dragon C dragon In dragon M dragon W 017, APC 096AU, I 9207C, M 9650, MS 3996AU, 174A, QC 377, QC 45, SDM 45, SDM 50, SMS	set lenguto, ompute, onsume on	th in  ity, ity, I IOT, I IOT, Music in  06, 07, , T, AU, CS605, M710, 150, R2130	pany/sct-securite lletins ber-20 bulleti	ty/bu /octo 119-		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID: CVE-2019-2268		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM650, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDX2- 031219/978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130		
			CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289	https://www.qualcomm.com/company/prodict-security/bulletins/october-2019-bulletin	H-QUA-SDX2- 031219/979
CV Scoring Scal	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

(CVSS)

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while standa user s Auto, s Electr Snapd Snapd Snapd Infras Netwo APQ80 IPQ40 MDM9 MDM9 MDM9 MSM8 QCA65 QCA65 QCS40 SDA84 SDM8 SM815	roverflooprocess, and NAN pace, in Snapdra onics Coloragon In Iragon Wiragon Wiragon, Miragon Wiragon, Miragon Wiragon, Miragon, Miragon, Miragon, Wiragon, Wirago	ing non- imessage Snapdra igon Cor onsume idustria Mobile, Toice & Movired e and 28053, 28096A; B064, IP DM964C SM8905 QCA617 QCA617 QCA937 N7605, S05, SDA 636, SDI 20, SDX	ge from agon asumer ity, r IOT, l IOT	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, 3 Snapd Snapd Mobile Music Weara APQ80 APQ80	P modulout side it receives essage. Is Snapdra Iragon Icagon Icag	its bour res malfo in Snapo agon Cor onsume ndustria oT, Snap dragon V ragon APQ800 Q8053, APQ809	ndary ormed dragon npute, r IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2303		
mdm9150					
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/982

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8933, MSM8940, MSM8953, MSM8996, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA65, SDM60, SDM710, SDM660, SDM670, SDM710, SM8250, SXR2130  CVE ID : CVE-2019-10490  SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8093, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9635, MDM9625, MDM9635M, MDM9640, MDM9655, MSM8909, MSM893, MSM8909, MSM893, MSM8909, MSM893, MSM8909, MSM8933, MSM8976, MSM8933, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM430, SDM450, SDM630, SDM632,  CV Scoring Scale  D1 12 23 33 34 45 56 672 788 889 340	Weakness	Publish Date	cvss	Description & CVE ID			Pat	ch	NCIIP	CID	
Out-of-bounds Read  Out-of				MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM8 SM61 SM82	3909, MS 3917, MS 3937, MS 3940, MS 3998, Nio 60, SDM 660, SDM 445, SDX 50, SM7	5M8909 5M8920, 5M8939, 5M8953, 5M8996, cobar, Q 2670, SD 20, SDX 2130	AU, CS605, M450, M710, 24, 8150,				
-		21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Mobil Music Wears APQ8 MDM' MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8	array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,				com /com produ ty/bu /octo	MDM9-	/983
(CVSS) 0-1 1-2 2-3 3-4 4-3 3-0 0-7 7-8 8-9 9-10	_	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID				Pat	ch	NCIIP	CID
			SDM7 SDX2 SM61 SM82 Snapo	36, SDM 10, SDX24 50, SM7 50, dragon_H 1130, SX <b>D : CVE-</b>	1845, SD 1, SDX55 150, SM High_Me R2130	M850, 8150, d_2016				
N/A	21-11-2019	7.2	copy is to the Paramare from Environment of Snapor	e invoking from fd of secure lands and comment. Snapdra dragon of dragon of dragon of dragon of tructure orking in 017, APO 098, MD 9205, MS 3996AU, 04, QCS 60, SDA 632, SDA	or local labuffer, eing popsecure in Snapelagon Cortonsume adustria Mobile, Vired and APQ80 Q8053, Q8096A PM9150, DM9206 DM9650 GM8909, GM8940, GM8940	ouffer oulated dragon inpute, vity, in IOT, loot, loot	https:/w.qualm.com pany/jct-securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- MDM9- 031219	/984
CV Scoring Scal	e 0.4	1.2					6.7	7.0	0.0	0.10
(CVSS)	0-1	1-2	2-3	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-2019-2315		
mdm9640					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MDM9- 031219/985

Weakness	Publish Date	CVSS	l	Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack o will be modificated bound Auto, Electron Snape Snape Snape Mobil Musico Wears APQ8 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDM2 SDM4 SDM4 SDM6 SDM7 SDX24 SM81	condition f resource e concur fied in the nent lead d access a Snapdra fonics Con dragon In dragon In drag	ce lock verently e memorals to out in Snapo gon Componnective onsume industria oT, Snap ragon Veragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905 MSM8906 MSM890	which  py t of dragon issumer ity, r IOT, dragon oice &  9,  8, 7C, 9, 89, AU, CS605, 845, M630, M660, X20, 150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in				https://w.qualm.com/pany/jct-securitelletins/ber-20	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID			Pat	ch	NCIIP	C ID	
			APQ8 APQ8 MDM' MSM8 MSM8 MSM8 MSM8 QCN7 SDM6 SDX2		Q8096A M9206, MDM960 DM9650 SM8909, MSM891 SM8953, MSM89 A660, SI	07, 0, 17, 98, 0M450, M660,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8996AU, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	/988
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto,			https://w.qual m.com pany/j ct- securit	com /com produ	H-QUA- MDM9- 031219		
CV Scoring Scal (CVSS)	e 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6		6-7	7-8	8-9	9-10		

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	PC ID
			Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDM6 SDM7 SDM2 SM61 SM82 Snapo Snapo	dragon C dragon In dragon In dragon In dragon In e, Snapdr ables in A 017, APC 096AU, A 9150, MI 9615, MI 9635M, I 9635M, I 9650, MI 3905, MS 3909W, I 3905, MS 3939, MS 3939, MS 3953,	ompute, onsume industria oT, Snap dragon Vagon APQ800 Q8053, APQ809 DM9605 DM8906 DM9605 DM9606 DM96	r IOT, l IOT, dragon oice & 9, 8, 40, 40, 7, 40, M439, M632, M670, M850, , 8150,	lletins, ber-20 bulleti	19-		
Improper Authenticati on	21-11-2019	10	allow NAS n result bypas Snapo Snapo Snapo	of integriss MODEN nessages into aut is of NAS dragon A dragon C dragon C	M to accommodate which of the conticate of the conticate of the continuation of the co	ept any can cion r IOT,	https://w.qual m.com pany/j ct- securit lletins/ ber-20	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			Mobil Music Wear: APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	lragon Ide, Snapdon, Snapdon, Snapdon, Apoles in Apoles in Apoles, Miles, Miles, Miles, Miles, Miles, Miles, Son, Miles, Son, Son, Son, Son, Son, Son, Son, Son	ragon V ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MB9676, MSM8937, SM8940, SM8976, MSM8937, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDA 6660, SD 6660, SD 845, SD 845, SD 845, SD 845, SD 845, SD 845, SD 845, SD 845, SD	oice & 9, 8, 5, 40, 5, 4660, M439, M632, M670, M850, 7, 8150, 612016	bulleti	n		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user s Auto, Electr Snapo Snapo Snapo Snapo Snapo	r overflo processi ard NAN pace. in Snapdra ronics Co Iragon In Iragon W Iragon W Iragon W tructure	ing non- messag Snapdra gon Cor onsume ndustria Iobile, oice & M	ge from agon asumer ity, r IOT, l IOT,	https:/ w.qual m.com pany/ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 APQ8 IPQ40 MDM9 MDM9 MSM8 QCA6 QCA9 QCS40 SDA8 SDM8 SM81		Q8053, Q8096A\ Q8096A\ QM9207 QM9640 GM8905 QCA617 QCA937 N7605, O5, SDA 636, SDI 20, SDX2	U, Q8074, C, , , , , , , , , , , , , , , , , ,				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear; APQ8 APQ8 MDM' MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MS	P modul out side it receive lessage. is Snapdra dragon In dragon I	e may active malforms	ccess idary ormed dragon inpute, r IOT, dragon oice &  9,  8,  40,  7,  77,	https:/w.qualm.com pany/jct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	/992
CV Scoring Scale	e <b>0-1</b>	1-2	2-3	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, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID: CVE-2019-2303		
mdm9650			0.2.2.10.10.2.013		
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8933, MSM8976, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MDM9- 031219/993

Weakness	Publish Date	CVSS	[	Description	n & CVE	ID	Pat	ch	NCIIF	C ID
			SDM8 SDX5! SM81 Snapd	60, SDM 45, SDM 5, SM615 50, SM82 dragon_H 130, SX	850, SD 50, SM7 250, Iigh_Me R2130	X20, 150, d_2016				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race of lack of will be modificated bound of Auto, Electron Snaped Snaped Mobil Musico Wears APQ8 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81	condition f resource e concur fied in the nent lead d access: Snapdra dragon Id dragon Id dragon Id dragon Id e, Snapdra dlagon Id dlagon	n due to ce lock we rently e memo ds to out in Snapo onnective onsume dustria oT, Snapo ragon V ragon APQ809 DM9207 DM9207 DM9640 SM8905 MSM893 SM8996 cobar, S405, Q0 60, SDA (439, SD (636, SD (636, SD	the which apy tof dragon assumer ity, ar IOT, adragon foice & 9, 8, 7C, 9, 89, AU, CS605, 845, M630, M660, X20, 150,	https://w.qualm.com/pany/jct-securitelletins/ber-20/bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	
Use After Free	21-11-2019	2.1	daem	QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150  CVE ID: CVE-2019-10486  Use after free issue in Xtra daemon shutdown due to static object instance getting  m.com/com					H-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

C 1 C	otion & CVE ID Patch NCIIPC ID
in Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Mobile, Sna Music, Snaj Wearables APQ8017, APQ8096A MDM9150 MDM9207 MDM9650 MSM8909, MSM8917, MSM8940, MSM8940, MSM898, SDA660, SI SDM660, SI SDM660, SI SDM660, SI SDM660, SI SDM845, SI SM8250, SI SM8250, SI SM8250, SI	security/bu lletins/octo ber-2019-bulletin lloT, a Industrial IOT, a IoT, Snapdragon pdragon Voice & odragon in APQ8009, APQ8053, J., APQ8098, MDM9206, C., MDM9607, MSM8905, MSM8909W, MSM8939, MSM8939, MSM8953, MSM896AU, Nicobar, QCS605, PA845, SDM450, DM670, SDM710, DX20, SDX24, M7150, SM8150,
Improper Validation of Array Index  21-11-2019 Array Index  occur in cat to imprope array index  Auto, Snap Electronics Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago	nds access can mera driver due r validation of in Snapdragon dragon Consumer Connectivity, n Consumer IOT, n Industrial IOT, n Mobile, n Voice & Music, n Wearables in  https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin
APQ8009,	APQ8017, APQ8096AU,

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID: CVE-2019-10503				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/997		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in	https://ww w.qualcom m.com/com pany/produ	H-QUA- MDM9- 031219/998		
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM9 MDM9 MSM8 QCA6 QCA9 SDA66 SDM6	lragon A lragon C onics Co lragon C lragon M lragon W 009, APC 053, APC 098, MD 9650, MS 3998, QC 574AU, C 379, QC 560, SDM 45, SDM	onsume onnectivonsume ndustria lobile, oice & M 28017, 28096A M9206, MDM960 SM8996 A6174A QCA937 S405, QO	ity, er IOT, el IOT,  Music in  U,  7, AU, 7, CS605, M636, M710,	ct- securii lletins ber-20 bulleti	/octo )19-		
Out-of- bounds Read	21-11-2019	10	Buffer while session messar un-interpretation of the session messar of the session of the sessio	D: CVE- r over re parsing n manage ges if ne tended v lragon A lragon C lragon Ic lragon Ic ge, Snapdr ables in A 017, APC 096AU, A 0150, MI 0206, MI 0206, MI 0635M, I 0635M, I 0635M, I 0635M, I 0635M, I 0635M, I 0639W, I	ad can had can	nappen nk OTA sends or IOT, l IOT, odragon oice & o o o o o o o o o o o o o o o o o o o	https:/ w.qual m.com pany/j ct- securir lletins ber-20 bulleti	ty/bu /octo	H-QUA- MDM9- 031219	/999
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	lragon_F l 130, SX	SM8940, SM8976, MSM89 2150, Qu 30X, SDA 429, SDI 630, SD 6660, SD 845, SD 5, SDX55 150, SM	98, CS605, A660, M439, M632, M670, M850, ,				
				<b>D</b> : <b>CVE</b> - of integri						
Improper Authenticati on	21-11-2019	10	NAS mesulta bypas Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8 MSM8	s MODEN nessages into aut is of NAS dragon A dragon C dragon In dragon Ic dragon Ic s, Snapdr ables in A 017, APC 096AU, A 9150, MI 9615, MI 9635M, I 9635M, I 89650, MS 8905, MS 8905, MS	s which of thentical in uto, ompute, onsume of the theorem of the	can tion  r IOT, l IOT, dragon oice &  9,  8,  6,  7,  40,  6,	https:/ w.qual m.com pany/i ct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- MDM9- 031219	/1000
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	1	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, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130			
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9650, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297	https://w.qualcom.com/opany/prct-security/lletins/ober-2010bulletin	om com rodu /bu octo	H-QUA- MDM9- 031219/100
CV Scoring Scal	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

(CVSS)

Weakness	Publish Date	CVSS	I	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snape Snape Snape Mobil Music Weara APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modulout side it receive lessage. Snapdra dragon Idragon Idragon, Mil 19635M, Idragon, Mil 19635M, Idragon, SDM 19635M, Idragon, SDM 19635, SC81845, SDM 19635, SC81845, SDM 196350, SDM	its bour res malfo in Snapo agon Cor onsume dustria oT, Snap ragon V ragon APQ800 Q8053, APQ809 DM9605 DM9625 DM9625 DM9655 SM8909, MSM891 SM8937, SM8940, SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MS	ndary ormed dragon inpute, er IOT, il IOT, idragon foice & 19, 8, 5, 7, 6, 40, 5, 6, 40, 6, 6, 4660, M439, M632, M670, M850, 6, 8150, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	/1002
N/A	21-11-2019	7.2	copy f to the Paran	invoking from fd of secure leters become non in the security of the security o	or local bouffer, eing pop	ouffer	https:/ w.qual m.com pany/j	com /com	H-QUA- MDM9- 031219	/1003
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Auto, Snapo Snapo Snapo Snapo Snapo Snapo Infras Netw APQ8 APQ8 APQ8 MDM MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6	onment. Snapdradragon Clagon Indragon I	igon Cor connective consume industria Mobile, Yoice & M Vired e and in APQ80 Q8053, Q8096A M9150, DM9206 DM9650 SM8940, SM8996, MSM86, MSM896, MSM86, MSM86, MSM86, MS	npute, vity, or IOT, l IOT, l IOT,  09, U, 5, 0, 4215, M429, M630, M660, M845, 7150, d_2016	securit lletins, ber-20 bulleti	octo 19-		
sdx24										
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	lack of array image Snapo Snapo Snapo Snapo	f bound of check of size white elf segn dragon Caragon Caragon Caragon Caragon I	of whilte ile readi nents. in auto, ompute onnectiv	elist ng the , vity, or IOT,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	/com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDM845, SDM870, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130   CVE ID : CVE-2019-2339   CVE ID : CVE-2019-2339	Weakness	Publish Date	CVSS	Description & C	/E ID	Pat	ch	NCIIP	C ID
lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8905, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QC				Snapdragon Wired Infrastructure and Networking in MDN QCS404, QCS605, SI SDM670, SDM710, SI SDM850, SDX24, SI SM6150, SM7150, SI SXR1130, SXR2130	19205, DA845, SDM845, IX55, M8150,				
	check Time- of-use (TOCTOU) Race	21-11-2019	4.4	lack of resource loc will be concurrently modified in the men statement leads to of bound access in Sna Auto, Snapdragon C Electronics Connect Snapdragon Industr Snapdragon Industr Snapdragon IoT, Sna Mobile, Snapdragon Wearables in APQ8 APQ8017, APQ8053 APQ8096AU, APQ8 MDM9206, MDM92 MDM9607, MDM96 MDM9650, MSM89 MSM8909W, MSM89 MSM8953, MSM899 MSM8953, MSM899 MSM8998, Nicobary QCN7605, QCS405, QM215, SDA660, SI SDM429, SDM439, S SDM429, SDM636, S SDM710, SDM845, S SDX24, SM6150, SM SM8150	k which concepy cut of	w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	_	

(CVSS)

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Use After Free	21-11-2019	2.1	daemstatic freed in Snape Snap	ter free on shutd object in from a mapdragon Chagon Chagon In the control of the	lown duastance and altiple in Auto, ompute onnectionsume adustria oT, Snap ragon Vagon APQ800 (SM8905) (SM8905) (SM8905) (SM8905) (SM8939, SM8939, SM8953, SM8	e to getting places  vity, or IOT, lIOT, dragon foice &  9,  8,  7,  W,  AU, CS605, M450, M710, 24, 8150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Out-of- bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
			APQ8 MSM8 QCN7 SDA6	lragon V 053, AP( 3996AU, 605, QC 60, SDM 0, SDX24	Q8096A MSM89 S405, Q0 636, SDI	U, 98, CS605,				
			CVE I	D : CVE-	2019-1	0563				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from source that the potent buffer Snape S	tmap file any un-a e, there he bitma tially can r overflo dragon C dragon C dragon C dragon In dragon W 016, APO 098, MD 098, MD 659, SC8 45, SDM 660, SDM 645, SDM 50, SM7 50, SM7	is a poss up can use stack w. in auto, compute connectiv consume consume consume dustria Mobile, M9205, M9205, M9205, MSM89 MSM	cated dibility k  vity, r ity, r IOT, l IOT,	https://w.qualm.com pany/jct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo 119- n	H-QUA- 031219	
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT,				https:/ w.qual m.com pany/j ct- securit lletins	com /com produ ty/bu	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Mobil Music Wears Wired Netwo IPQ40 MDM9 MSM8 QCA9 SDM8 SM81	dragon Idee, Snapdrables, Snapd	ragon V ragon apdrago ructure a APQ80 3064, DM9207 SM8909 Nicobar, S405, Q0	oice & on and 53, CC, , 2S605, 150,	ber-20 bulleti			
Out-of- bounds Read	21-11-2019	10	while session messar un-information of Snapor Snapor Snapor Snapor Snapor Snapor Snapor Snapor Snapor Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8 MSM8	r over reparsing manages if netended valuagen Caragon Caragon Interpretation and pages in Augusta 1960, Miles in A	downlingement (etwork stralues in uto, ompute onsume ndustria oT, Snaperagon Vagon APQ800 Q8053, APQ809 DM9607 DM9605 DM8900 DM8	nk OTA Sends  r IOT, l IOT, dragon oice &  9,  8,  7,  40,  5,  47,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-9	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			SDA8- SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	.5, SC818 45, SDM 50, SDM 10, SDM 0, SDX24 50, SM7: 50, dragon_H 130, SX	429, SDI 630, SD 660, SD 845, SD 5, SDX55 150, SM ligh_Me R2130	M439, M632, M670, M850, , 8150, d_2016				
Improper Authenticati on	21-11-2019	10	Lack of allow. NAS in result bypas Snapo Snapo Snapo Snapo Snapo Mobil Music Wear; APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integris MODEN nessages into aut is of NAS dragon A dragon C dragon In dragon In dragon In 19635M, In 19635	ity check M to accombined to hentical in uto, ompute, onsume adustria oT, Snap ragon APQ800 Q8053, APQ809, APQ809, A	ept any can tion  r IOT, l IOT, dragon oice & 9, 8, 5, 7, 6, 40, 6, 7, 17, 17, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-3 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID				Pat	ch	NCIIP	C ID			
			SDM7 SDX2 SM61 SM82 Snapo	36, SDM 10, SDX24 50, SM7 50, dragon_H 1130, SX <b>D : CVE-</b>	1845, SD 1, SDX55 150, SM High_Me R2130	M850, , 8150, d_2016							
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electric Snape Snape Snape Snape Infrast APQ8 APQ8 IPQ40 MDM MDM MDM MSM8 QCA6 QCA9 QCS40 SDA8 SDM8	Buffer overflow can occur while processing non- standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150				//ww com /com produ ty/bu /octo 19- n	H-QUA- 031219				
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute,				array out side its boundary when it receives malformed XID message. in Snapdragon w.qualcom m.com/com pany/produ H-QUA-SDX2 031219/101			undary w.qualcom formed m.com/com odragon pany/produ			
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10			

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	security/bu lletins/octo ber-2019- bulletin	
			CVE ID : CVE-2019-2303		
ipq4019					
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-	H-QUA-IPQ4- 031219/1014
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID: CVE-2019-2266	bulletin	
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297	https://ww w.qualcom m.com/com pany/produ ct- security/bu	H-QUA-IPQ4- 031219/1015
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
ipq8064					
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150  CVE ID: CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-IPQ8- 031219/1016
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-IPQ8- 031219/1017

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Pu	blish Date	cvss	Description & CVE ID				Pat	tch	NCIIP	C ID
				MSM8 QCA6 QCA9 QCS4 SDA8 SDM8 SM81	MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID: CVE-2019-2297						
				CVE I	D : CVE-	2019-2	297				
ipq8074											
Integer Underflow (Wrap or Wraparound )	21-	-11-2019	4.6	while stand user stand user stand user stand user stand user stand	r overfloor process and NAN space, in Snapdra conics Codragon Indragon Indragon Vertructure orking in 017, APO 19, IPQ 9206, M. 9650, M. 574AU, 379, QC 19, SDX 19, SD	ing non- I message Snapdra agon Cor connective consume ndustria Mobile, Vired e and n APQ80 Q8053, Q8096A 8064, IP DM9640 SM8905 QCA617 QCA937 N7605, 605, SDA 636, SDA	ge from agon issumer rity, er IOT, ll	https:/w.qualm.com pany/ct- securilletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	•
Out-of- bounds Read	21-	-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary				https:/ w.qua	lcom	031219/1019	
CV Scoring Scal (CVSS)	e	0-1	1-2	memo	ory read 3-4	which v	vill 5-6	m.com	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318	pany/produ ct- security/bu lletins/octo ber-2019- bulletin	
qca6174a			Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCA6- 031219/1020

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150  CVE ID: CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA6- 031219/1021
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing non- standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCA6- 031219/1022
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	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, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150		
g g 0 2 7 7			CVE ID : CVE-2019-2297		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCA9- 031219/1023

4-5

6-7

7-8

8-9

9-10

5-6

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130		
			CVE ID : CVE-2019-10566		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCA9- 031219/1024
			CVE ID : CVE-2019-2268		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing non- standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA9- 031219/1025
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish	Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	CID
				MDM' MDM' MSM8 QCA6 QCA9 QCS4 SDA8 SDM8	019, IPQ 9206, M 9607, M 9650, M 3996AU, 574AU, 379, QC 05, QCS6 45, SDM 445, SDX 50	DM9207 DM9640 SM8905 QCA617 QCA937 N7605, 605, SDA 636, SDI 20, SDX2	7C, 74A, 77, 660, M660,				
qca9379				CVEI	D : CVE-	2019-2	Z9 /				
					r overflo						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-	2019	4.6	rates eleme than in Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81 CVE I	module in or extendent length max rate dragon Adragon Conics Colleagon Magon Work, APO 174A, Quantum	ded rate h is grea set leng uto, ompute onsume onsume onsume dustria lobile, loice & M Q8053, MDM920 MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0 670, SDI 20, SM6 250, SXI 2019-1	es atter (th in ), r (th in ),	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com orodu cy/bu /octo 19-	H-QUA-0 031219,	-
Out-of-	21-11-	2019	7.5		Possible 00B read issue in P2P action frames while			https:/ w.qual	•	H-QUA-0	QCA9-
CV Scoring Scale (CVSS)	e 0-	-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
bounds Read			mana Snapo Snapo Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM' MDM' MSM8 QCA6 QCA9 SDA6 SDM6 SDM8	ing WLA gement for agon A dragon Conics Cooling on Ir dragon Ir dragon Ir dragon V 009, APO 053, APO 098, MD 9207C, M 9650, MS 574AU, O 379, QCS 60, SDM 660, SDM 645, SDX	frame in uto, onsume onnectivonsume dustria dobile, foice & MQ8017, Q8096A M9206, MDM960 SM8996 A6174A QCA937 S405, QCA957	or ity, or IOT, I IOT, Music in U, O7, AU, A, 7, CS605, M636, M710, 150	m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	031219	/1027
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electric Snapo Snapo Snapo Infras Netwo APQ8 APQ8 IPQ40 MDM MDM MDM MDM MDM	r overflo processi ard NAN space. in Snapdra conics Co dragon In dragon I dragon V dragon V dragon V dragon V dragon V dragon V dragon W 194, APO 19, IPQ8 9206, MI 9650, MS	ing non- message Snapdra gon Cor onnective onsume ndustria fobile, foice & M Vired and APQ80 Q8053, Q8096A B064, IP DM9207 DM9640	ge from agon asumer ity, or IOT, l IO	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-031219	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID: CVE-2019-2297		
snapdragon l	 high_med_201	6	CVE ID . CVE-2017-2277		
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SNAP- 031219/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM8953, MSM8976, MSM8953, MSM8976, MSM8953, MSM8976, SM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SNAP- 031219/1030

Weakness	Publish Date	cvss	Description & CVE ID	Patch	1	NCIIP	C ID
			, SXR1130, SXR2130				
			CVE ID : CVE-2019-2271				
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289	https://w.qualcom.com/opany/proct-security/lletins/ober-201bulletin	om com rodu /bu octo	H-QUA-3 031219	
CV Scoring Scal	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	:ch	NCIIF	PC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape SDM6 SDM6 SDM6 SDM6 SDM8 Snape , SXR1	lragon_H	ress range the Systode. in uto, ompute onnectivonsume dustria lobile, oice & Marcolon (2005), 600, 600, 600, 500, 500, 500, 500, 500	ge DBG  vity, r IOT, l IOT, 4usic, 09, , CS404, 215, M429, M630, M660, M845, d_2016	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. 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://w.qualm.com pany/jct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch.	NCIIP	CID
			MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM7 SDX2 SM61 SM82 Snapo , SXR1	096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MI 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 3053, MS 3075, SDM 450, SDM 450, SDM 50, SDX24 50, SM7 50, Iragon_H 1130, SXI D: CVE-	DM9205 DM9607 DM9625 MDM964 DM9655 M8909, MSM891 SM8976, MSM8976, MSM89 2150, Q0 30X, SDA 429, SDA 660, SD 660, SD 6845, SD 660, SD 6845, SD	5, 7, 6, 40, 6, 40, 7, 7, 27, 28, 28, 28, 28, 38, 46, 46, 48, 48, 50, 61, 61, 61, 61, 61, 61, 61, 61, 61, 61				
N/A	21-11-2019	7.2	copy to the Paran are from environment of Snapo	e invoking from fd of a secure be neters be om non somment. Snapdradragon Colragon Colragon Wolragon W	or local bouffer, eing popsecure in Snapegon Coronsumendustria lobile, foice & March 1980 (1980) (19	ouffer oulated dragon npute, vity, r IOT, l IOT, fusic,	https://w.qualm.com pany/jct- securite lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130		
Out-of- bounds Read	21-11-2019	2.1	CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SNAP- 031219/1035

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			CVE I	D : CVE-	2019-2	318				
apq8009										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi result in Sna Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	e process t messag tion is no cing into apdragon C dragon In drago	te, Valid of met an infin in Auto, ompute onsume industria oT, Snapparagon Vagon APQ800 DM9607 DM9607 DM9605 SM8909, MSM8913, SM8953,	exit ite loop , er IOT, l IOT, dragon foice &  9,  8, 5, 7, 6, 17, AU, M215, A845, M450, M636, M710, X20, 150, d_2016	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	_
Time-of-	21-11-2019	4.4		conditio			https:/	•	H-QUA- 031219	-
check Time-			iack o	f resour	ce lock v	vnicn	w.qual	com	031419	/ 103/
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

of-use (TOCTOU) Race Condition  will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, bulletin	
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, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID: CVE-2019-10486	
Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon ber-2019-  Use after free issue in Xtra daemon shutdown due to static object instance getting https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-	•
Mobile, Snapdragon Voice & bulletin Music, Snapdragon Wearables in APQ8009,	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130  CVE ID: CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM896AU, MSM8988, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8- 031219/1039

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch:	NCIIP	C ID
			SDX2	0						
			CVE I	D : CVE-	2019-1	0503				
Out-of- bounds Read	21-11-2019	7.5	P2P a handle mana Snape Snape Snape Snape APQ8 APQ8 MDM MSM8 QCA6 QCA9 SDA6 SDM8	ble OOB ction fra ing WLA gement dragon A dragon C dragon I dragon W dragon W 009, AP 053, AP 098, MD 9207C, M 9650, M 574AU, 379, QC 574AU, 379, QC 60, SDM 660, SDM 645, SDX D: CVE-	imes whan frame in tuto, consume connective consume dobile, Coice & M Q8017, Q8096A M9206, MDM960 SM8996 CA6174A QCA937 S405, QC 630, SD 1670, SD 20, SM6	r ity, r IOT, l IOT, fusic in U, AU, 7, CS605, M636, M710, 150	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- 031219	-
Out-of- bounds Read	21-11-2019	10	while session messaun-in Snapo Snapo Snapo Mobil Music Wear APQ8	parsing parsing on manages if no dragon Adragon Idragon Idrago	downlingement etwork stralues in auto, compute on sume of the consumer of the	nk OTA eends r IOT, l IOT, dragon oice &	https://w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com l/com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal	e 0.4	1.2	2.2	2.4	4.5	F. C	6.7	7.0		0.40
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	9150, MI 9206, MI 9615, MI 9635M, I 9650, MI 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3953, MS 3953, MS 36, SDM 45, SC818 45, SDM 45, SDM 50, SDX24 50, SM7 50, SM7 50, SM7	DM9607 DM9625 MDM9655 SM8909, MSM891 SM8940, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDI 1630, SD 1845, SD 150, SM High_Me R2130	98, CS605, M660, M439, M670, M850, M62016				
Improper Authenticati on	21-11-2019	10	allow NAS result bypas Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM	of integrals MODE! nessages into autoris of NAS dragon A dragon C dragon In dragon Io c, Snapdr ables in A 017, APO 096AU, A 9150, MI 9206, MI	M to accombined	ept any can cion r IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			MDM <sup>o</sup> MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	dragon_H 1130, SX	DM9655 M8909, MSM8937, SM8940, SM8976, MSM89 2150, Q 30X, SD 429, SD 660, SD 660, SD 845, SD 750, SM	5, 17, 198, CS605, A660, M439, M632, M670, M850, 5,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information lack check buffer Snape	D: CVE- mation d k of addr done on rs in SDI dragon A dragon C dragon C dragon W dragon W dragon W dragon W structure orking in 017, APO 89205, MS 8920, MS 8940, MS	isclosures range the System on sume on	re due ge sDBG  vity, er IOT, l IOT, Music, 09,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	_
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pul	olish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
				SDM4 SDM6 SDM6 SDM8 Snapo , SXR1	lragon_I l 130 <b>D : CVE-</b>	1450, SD 1636, SD 1710, SD High_Me <b>2019-2</b>	M630, M660, M845, d_2016				
Integer Underflow (Wrap or Wraparound )	21-	11-2019	4.6	while stand user's Auto, Electric Snape Snape Snape Snape Infrast APQ8 APQ8 IPQ40 MDM MDM MDM MDM MSM8 QCA6 QCA9 QCS40 SDA8 SDM8 SM81	r overflooprocess and NAN space. in Snapdra onics Coloragon I dragon I dragon Vertructure orking in 017, APO 064, APO 019, IPQO 9206, ME 9650, ME 9	ing non- imessage Snapdra igon Cor onnective consume industria Mobile, Vired e and in APQ80 Q8053, Q8096A B064, IP DM9640 SM8905 QCA617 QCA937 N7605, 505, SDA 636, SDA	ge from agon asumer ity, r IOT, l IOT	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	-
Out-of- bounds Read	21-	11-2019	7.5	array when XID m	SNDCP module may access https:// array out side its boundary w.qualcomen it receives malformed m.com/ XID message. in Snapdragon pany/product.		com /com	H-QUA- 031219	-		
CV Scoring Scal (CVSS)	е	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Snapo Mobil Music Wear; APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	dragon Coloragon Infragon Infr	ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9607 DM9625 MDM9655 SM8909, MSM891 SM8937, SM8940, SM8976, MSM8937, SM8940, SM8976, MSM891 EMSM8937, SM8955 SM8976, MSM8937, SM8937, SM	1 IOT, dragon foice & 9, 8, 5, 7, 5, 40, 5, 40, 65, 4660, M439, M632, M670, M850, 6, 8150, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	securit lletins, ber-20 bulleti	octo 19-		
N/A	21-11-2019	7.2	copy for the to the Paran are from the environment of the Environment	e invokin from fd o secure l neters be om non s onment. Snapdra dragon C dragon I	or local buffer, eing popsecure in Snapelgon Corlonnectivons under the consume	ouffer oulated dragon mpute, vity, er IOT,	https://w.qual m.com pany/p ct- securit lletins, ber-20 bulleti	com /com orodu cy/bu /octo 19-	H-QUA- 031219	-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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, MSM8953, MSM8996, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
apq8098					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-APQ8- 031219/1047

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch.	NCIIP	CID
			MDM <sup>o</sup> MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> SC818 SC818 SDM <sup>o</sup> SDM <sup></sup>	9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 9650, MS 3905, MS 3998, MS 3976, MS 3998, Nic 2150, QC 30X, SDA 450, SDM 50, SDM 50, SDM 50, SDM 50, SM615 1130, SX D: CVE-	DM9607 DM9625 MDM9655 SM8909, MSM8915 SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8975 SM8975 SM8975 SM8975 SM8975 SM8975 SM8975	M215, A845, M450, M710, X20, M2016				
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modified stater bound Auto, Electric Snape Snape Mobil Music Wears APQ8 APQ8 MDM MDM MDM	condition of resource e concur- fied in the ment lead d access Snapdra conics Co dragon I dragon I dra	ce lock werently the memorals to our in Snaper in Snaper in Snaper industria oT, Snaper iragon V ragon APQ800 Q8053, APQ809 DM9640	which  py t of dragon isumer ity, or IOT, l IOT, odragon oice &  9,  8, 7C,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID: CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-APQ8- 031219/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM896AU, MSM898, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-APQ8- 031219/1050
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, 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/october-2019-bulletin	H-QUA-APQ8- 031219/1051

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 QCA6 QCS4	098, MD 3996AU, 574AU, ( 05, QCS6 45, SDX	MSM89 QCN760 505, SDA	98, 5,				
			CVE I	D : CVE-	2019-1	0535				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from a source that the potent buffer Snape	tmap file any un-a e, there is he bitma tially can roverflo dragon A dragon C dragon C dragon In dragon V 016, APO 098, MD 3996AU, ar, QCS4 55P, SC8 45, SDM 60, SDM 60, SDM 50, SM7 50, SM7	authenticis a possip can use stack w. in auto, compute connective consume ndustria Mobile, Moice & Monga Mos	cated dibility k  k  vity, r ity, r ity, l IOT, l I	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
Out-of- bounds Read	21-11-2019	7.5	P2P a handl mana Snapo Snapo Electr	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,		https://w.qual m.com pany/j ct- securit lletins/ ber-20	com /com produ ty/bu /octo	H-QUA- 031219	•	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	l	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo APQ8 APQ8 APQ8 MDM' MSM8 QCA6 QCA9 SDA6 SDM6	lragon Indragon Maragon Maragon Wallagon Wallagon Wallagon Wallagon Maragon Ma	Iobile, oice & M 28017, 28096A M9206, IDM960 SM8996 A6174A QCA937 S405, QC 630, SDI 670, SD	Music in U, 7, AU, 7, CS605, M636, M710,	bulleti	n		
Out-of- bounds Read	21-11-2019	10	while session messar un-interest snaped Snaped Snaped Snaped Snaped Mobil Music Wears APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	r over reparsing on manages if netended valuages if netended valuages if netended valuages in Adragon Caragon In Gragon In Gra	downlingement (extwork stalues in uto, ompute, onsume ndustria oT, Snaparagon Vagon APQ800 Q8053, APQ809 DM9625 DM9625 DM9625 DM9625 DM9625 DM9655 DM	nk OTA ends  r IOT, l IOT, dragon oice &  9,  8,  7,  40,  7,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130   CVE ID : CVE-2019-2271	Weakness	Publish Date	cvss	l	Description	n & CVE	ID	Pat	ch	NCIIP	CID
allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9625, MDM9615, MDM9625, MDM96040, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8937, MSM8939, MSM8940, MSM893, MSM8964, MSM8996AU, MSM8964, MSM8964, MSM8996AU, MSM8964, MSM89664, MSM89664, MSM8996, Nicobar, QCM215, SC8180X, SDA660, SDA845, SDM429, SDM439,				QM21 SDA8 SDM4 SDM7 SDX2 SM61 SM82 Snapo	.5, SC818 45, SDM .50, SDM .36, SDM .10, SDX24 50, SM7 50, dragon_H	80X, SDA 429, SDI 6630, SD 6660, SD 845, SD 150, SM High_Me R2130	A660, M439, M632, M670, M850, , 8150,				
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Authenticati	21-11-2019	10	allow NAS result bypas Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	s MODEl nessages into aut s of NAS dragon A dragon G dragon I dragon I dragon I dragon I gragon I grag	M to accombined	ept any can tion  r IOT, l IOT, dragon coice & 9, 8, 7, 7, 40, 6, 7, 100, 100, 100, 100, 100, 100, 100,	w.qual m.com pany/ ct- securi lletins ber-20	com /com produ ty/bu /octo	-	_
	CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	lragon_H 1130, SXI <b>D : CVE-</b>	660, SD 845, SD 5, SDX55 150, SM High_Me R2130 <b>2019-2</b>	M670, M850, , 8150, d_2016				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modul out side it received sage. It received sage. It received sage. It received sage in a section of the sage in a sec	its bour es malfo in Snapo gon Cor onsume dustria oT, Snap ragon V agon APQ809 DM9205 DM9607 DM9625 MDM9655 MB909, MSM891 SM8937, SM8940, SM8940, SM8976, MSM89 2150, Qu 30X, SD4 429, SD4 660, SD 660, SD 660, SD 845, SD	ndary ormed dragon inpute, in IOT, dragon foice & 9, 8, 5, 7, 7, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,	https:/w.qualm.com pany/jct-securifiletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

SM8250,   Snapdragon, High_Med_2016   , SXR1130, SXR2130	Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
N/A  21-11-2019  7.2  APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, MSM8998, QC\$404, QC\$605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  H-QUA-APQ8- 031219/1057	Weakness	Publish Date	CVSS	SM82 Snapo , SXR2 CVE I  While copy to the Paran are fr envire Auto, Snapo Sna	50, dragon_F 1130, SX D: CVE- e invoking from fd of e secure le eneters be om non se onment. Snapdra dragon Ce dragon Ce dragon We dragon V etructure orking ir	High_Me R2130  2019-2  g the AF or local brouffer, eing pope secure in Snape onnection on sume adustria fobile, foice & Mared and a APQ80	d_2016  303  PI to ouffer oulated dragon inpute, vity, or IOT, I IOT, I IOT, I IOT,	https:/	//ww	NCIIP	CID
msm8939		21-11-2019	7.2	APQ8 APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SM81 Snapo , SXR2	017, APC 096, APC 098, MD 9205, MS 9607, MS 3905, MS 3917, MS 3937, MS 3953, MS 3996AU, 04, QCS6 60, SDA8 439, SDM 532, SDM 532, SDM 550, SM6 50, SM6	Q8053, Q8096A M9150, DM9206 DM9650 SM8909, SM8940, SM8940, SM8946, MSM89 605, QM2 6450, SD 6450, SD 150, SM	U, 98, 215, 4429, M630, M660, M845, 7150, d_2016	w.qual m.com pany/ ct- securi lletins ber-20	com /com produ ty/bu /octo	_	_
	CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch	NCIII	PC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack o will be modificated bound Auto, Electric Snaped Snaped Snaped Mobilic Wears APQ86 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 SDM2 SDM4 SDM4 SDM4 SDM2 SM81	condition f resource e concur ied in the nent lead d access Snapdra conics Col lragon Id lragon Id e, Snapdra dlragon Id dlragon Id e, Snapdra dlragon Id dlragon Id	ce lock werently e memorish to our in Snape ingon Cor onsume industria oT, Snape ragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905 MSM8905 GM8905 GM8	which  apy t of dragon asumer aty, ar IOT, al IOT, adragon oice &  a, b, c, c, dragon oice & dragon	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
Use After Free	21-11-2019	2.1	daemo static freed in Sna Snapd Snapd Snapd Snapd Snapd	ter free on shute object ir from a napdragon Caragon Caragon Iragon Iragon Iragon Icagon Icag	lown dunstance in Auto, ompute onnectionsumendustria	e to getting places , vity, er IOT, l IOT, odragon	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			Wears APQ8 APQ8 MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61	c, Snapdrables in A 017, APC 096AU, A 9150, MI 9207C, M 9650, MS 3909, MS 3917, MS 3940, MS 3996, MS 3996, MS 3996, MS 3998, Nic 60, SDAS 50, SM7 50, SXR2	APQ800 Q8053, APQ809 DM9206 MB905 SM8905 SM8939, SM8939, SM8939, SM8953, SM8953, SM8953, SM8953, SM8958, SM8958, SM8958,	8, 5, 07, , W, CS605, M450, M710,				
			CVE I	D : CVE-	2019-1	0490				
Out-of- bounds Read	21-11-2019	10	while session messar un-information Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MDM MDM MD	r over reparsing on manages if netended valuagen Caragon Caragon Indragon I	downlingement of tworks alues in uto, ompute onsume ndustria oT, Snappragon Vagon APQ800 Q8053, APQ809 DM9607 DM9605 DM9605 SM8909, SM8909, SM8909, APQ809 DM9605 SM8909 DM9605 SM8900 S	nk OTA sends  or IOT, I IOT, dragon oice &  9,  8, 5, 40, 5,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1060
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	lragon_F l130, SX	SM8940, SM8976, MSM89 2150, Qu 30X, SDA 429, SDI 630, SD 6660, SD 845, SD 5, SDX55 150, SM	98, CS605, A660, M439, M632, M670, M850, ,				
			Lack	<b>D : CVE-</b> of integri	ity checl	ζ.				
Improper Authenticati on	21-11-2019	10	NAS mesulta bypas Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8 MSM8	s MODEN nessages into aut is of NAS dragon A dragon C dragon Ic dragon Ic dragon Ic e, Snapdr ables in A 017, APC 096AU, A 9150, MI 9206, MI 9635M, I 9635M, I 3905, MS 3909W, I 3909W, I 3920, MS	s which of thentical in uto, ompute, onsume of the theorem of the	r IOT, l IOT, dragon foice &  9,  8,  6,  7,  40,  6,	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1061
CV Scoring Scal (CVSS)	e <b>0</b> -1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			Nicob QM21 SDA8 SDM4 SDM7 SDX20 SM61 SM82 Snapo , SXR1	3996AU, ar, QCM 5, SC818 45, SDM 36, SDM 10, SDM 0, SDX24 50, SM7 50, lragon_H 130, SX <b>D: CVE-</b>	2150, Q0 30X, SDA 429, SDI 630, SD 6660, SD 845, SD 7, SDX55 150, SM High_Me R2130	CS605, A660, M439, M632, M670, M850, , 8150,				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear: APQ8 MDM' MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8	P modul out side it receiv lessage. Snapdra lragon Ic lragon Ic g, Snapdr ables in 1 017, APC 096AU, 1 9206, MI 9206, MI 9635M, I	e may active malforms	ccess idary ormed dragon inpute, r IOT, dragon oice &  9,  8,  6,  7,  7,  40,  6,  7,  40,  6,  7,  40,  6,  6,  6,  6,  6,  6,  6,  6,  6,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219,	/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID: CVE-2019-2303		
msm8953					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MSM8- 031219/1063

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SM81 Snapo	5, SM61! 50, SM8 lragon_F l130, SX	250, ligh_Me					
			CVE I	D : CVE-	2019-2	335				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated bound Auto, Electron Snape Snape Mobil Music Wears APQ8 MDM MDM MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX2 SM81	condition f resour fe concur fied in the ment lead d access Snapdra conics Col dragon In dragon	ce lock werently the memory in Snapelingon Corporative onsume andustria of Snapelinagon Veragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905 MSM8	which  apy t of dragon asumer aty, ar IOT, al IOT, adragon oice &  a9,  8, 7C, 0, , 39, AU, CS605, 845, M630, M660, X20, 150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1064
Use After Free	21-11-2019	2.1	Use at daem static freed	fter free on shute object in from a m	issue in lown du istance ; nultiple	Xtra e to getting	https:/ w.qual m.com pany/j	com /com	H-QUA- MSM8- 031219	/1065
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Snapo Snapo Snapo Mobil Musio Wears APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SM82	dragon C dragon C dragon I dragon I dragon I dragon I dragon I e, Snapdr ables in A 9150, MI 9207C, M 9650, MS 3909, MS 3909, MS 3917, MS 3937, MS 3940, MS 3996, MS 3997, MS 3998, Nice 3998,	connective on sume and ustrial off, Snap bragon APQ800 Q8053, APQ809 DM960 SM8905 SM8905 SM8939, SM8953, SM8956, SM895	vity, or IOT, ol IOT, olragon olice & 9, 8, 5, 77, , W, CS605, M450, M710, 24, 8150,	securit lletins ber-20 bulleti	/octo 19-		
Improper Validation of Array Index	21-11-2019	4.6	occur to imparray Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM	f-bounds in came proper v index in Snapdra ronics Co dragon C dragon W dragon W 009, APO 053, APO 098, MD 9207C, M	ra drive alidation Snapdr Igon Cor Innectiv Ionsume Industria Mobile, Yoice & M Vearable Q8017, Q8096A M9206, MDM960	r due n of agon nsumer ity, er IOT, I IOT, Usic, es in U,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			MSM8 MSM8 MSM8 MSM8 QCN7	3905, MS 3909W, I 3920, MS 3940, MS 3996AU, 605, SDM 30, SDM	MSM891 SM8937, SM8953, MSM89 A660, SI	17, 98, 0M450,				
			CVE I	D : CVE-	2019-1	0503				
Out-of- bounds Read	21-11-2019	10	while session messar un-interpretation of the session messar un-interpretation of the session messar un-interpretation of the session of the	r over reparsing on manages if netended valuagion Adragon Adragon Interpretation of the control	downlingement of the twork stalues in the two computers on sume adustria of the two consumers	nk OTA ends r IOT, I IOT, dragon oice & 9, 8, 6, 7, 6, 40, 6, 7, 17, 17, 18, 17, 18, 198, 198, 198, 198, 198, 198, 198,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- MSM8- 031219,	/1067
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SM61 SM82 Snapo , SXR2	0, SDX24 50, SM7 50, dragon_H 1130, SX <b>D : CVE-</b>	150, SM ligh_Me R2130	8150, d_2016				
Improper Authenticati on	21-11-2019	10	Lack of allow NAS result bypas Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integrals MODER nessages into autorise of NAS dragon A dragon A dragon I	ity check M to access which of thentical in auto, ompute, onsume adustria oT, Snap ragon V ragon APQ800 Q8053, APQ809 DM9607 DM9607 DM9607 DM9605 DM9607 DM9605 SM8909, MSM891 SM8937, SM8940, SM8940, SM8940, SM8940, SM8940, SM8940, SM8940, SM8953, MSM891 SM8937, SM8940, SM8940, SM8940, SM8940, SM8940, SM8953, SM8940, SM8953, SM8940, SM8953,	ept any can cion r IOT, l IOT, dragon oice & 9, 40, 7, 7, 4660, M439, M632, M670, M850, 7, 7,	https:/w.qualm.company/jct-securitletins/ber-20	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1068
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			^	lragon_F I 130, SX	•	d_2016				
			CVE I	D : CVE-	2019-2	289				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape	lragon_F L130	ress range the System the System the System to the System	ge sDBG , vity, or IOT, l IOT, Music, 09, , CS404, 215, M429, M630, M660, M845, d_2016	https://w.qualm.company/jct-securitelletins/ber-20bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1069
			CVE ID : CVE-2019-2295  SNDCP module may access		https:/	/ /ҳʌァҳʌァ				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo	array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon				com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDM7 SDM7 SDM2 SM61 SM82 Snapo	e, Snapdr e, Snapdr ables in 2 017, APC 096AU, 2 9150, MI 9635M, I 9635M, I 9650, MI 3905, MS 3909W, I 3996AU, ar, QCM -5, SC818 45, SDM -50, SDM 10, SDM 10, SDM 50, SM7 50, SM7 50, SM7	ragon APQ800 Q8053, APQ809 DM9607 DM9607 DM9655 MDM9655 SM8909, MSM891 SM8937, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDA 1660, SD 1660, SD 1845, SD 150, SM High_Me R2130	9, 8, 5, 40, 5, 40, 6, 17, 28, 4660, M439, M632, M670, M850, 6, 8150, d_2016	bulleti	n		
N/A	21-11-2019	7.2	copy for the the Param are from the environment of	e invoking from fd ( e secure le eneters be om non e onment. Snapdra dragon C dragon I dragon V dragon V	or local louffer, eing popsecure in Snapelgon Coronsumendustrialobile, foice & M	ouffer oulated dragon mpute, vity, r IOT, l IOT,	https:/ w.qual m.com pany/j ct- securif lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1071
CV Scoring Scal	e 0-1	1-2	Snapdragon Wired  2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10
(CVSS)										

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,					on & CVE		1 4	:ch	- IVCIII	CID
QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315			Netwo APQ8 APQ8 APQ8 MDM9 MSM8 MSM8 MSM8 QCS49 SDA69 SDM6 SDM6 SDM6 SDM6 SDM8 SM81 Snapo	orking ir 017, APC 096, APC 098, MD 9205, MI 3905, MS 3917, MS 3937, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 304, QCS6 304, QCS6 305, SDM 3070, SDM 3070, SDM 3070, SM6 3070, SM6	APQ80 Q8053, Q8096A M9150, DM9650 SM8909, SM8940, SM8940, SM8946, MSM89 605, QM2 845, SDM (450, SD (710, SD (710, SD (710, SM	U,  98,  215,  M429,  M630,  M660,  M845,  7150,  d_2016				
Out-of-bounds Read  21-11-2019  Out-of-bounds Read  Out-of-Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8917, MSM8940, MSM8940,	21-11-2019	2.1	Trusti memo result Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 APQ8 MSM8 MSM8	zone to o bry read dragon A dragon C dragon I dragon W dragon W dragon W dragon W dragon W dragon W 3933, APG 3937, MS	do an ari which w S in uto, onnective onsume ndustria Mobile, foice & M Vired and APQ80 Q8096, IPQ8074 SM8920, SM8940,	bitrary vill vity, r IOT, l IOT, fusic,	w.qual m.com pany/ ct- securi lletins ber-20	ty/bu /octo	MSM8-	/1072
MSM8953, MSM8996, MSM8996AU, QCA8081,	le 0.4		1 101.10	0110)	2311000	,	<u> </u>			9-10

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch:	NCIIP	CID
msm8998			SDM4 Snapo	5, SDM4 50, SDM lragon_H <b>D : CVE</b> -	632, Iigh_Me	d_2016				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condiresult in Snape Snape Snape Snape Snape Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	process the message tion is not ing into apdragon Ce dragon Ir dragon II dragon Ir dragon Ir dragon Ir dragon Ir dragon Ir dragon Ir dra	e, Valid of met an infin Auto, ompute onsume dustria oT, Snap ragon APQ800 (28053, APQ809 (250, MSM891) (3605, S) (3605, Q) (3605, Q) (3605, S) (3	exit ite loop , er IOT, l IOT, dragon oice & 9, 8, 5, 40, 6, 40, 6, 40, 6, 40, 6, 40, 6, 40, 6, 40, 6, 40, 6, 6, 40, 6, 6, 40, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			CVE I	D : CVE-	2019-2	335				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated bound Auto, Electron Snape Snape Snape Mobil Music Wears APQ8 MDM MDM MDM MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX2 SM81	condition f resour f resour e concur ied in the nent lead d access Snapdra dragon In dragon In dragon In dragon In dragon In dragon In dragon In e, Snapdra sbles in 017, APO 096AU, 2 9607, Mi 9650, Mi	ce lock verently te memorials to out in Snape of the consume of th	which  py t of dragon ity, r IOT, dragon oice &  9,  8, 7C, 0, , 89, AU, CS605, 845, M630, M660, X20, 150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1074
			_				httpg	/ / * * * * * * * * * * * * * * * * * *		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1075
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss		Descriptio	on & CVE	ID	Pat	ch:	NCIIP	C ID
			Mobil Music Wears APQ8 APQ8 MDM' MDM' MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM8	dragon Idee, Snapder, Snapdrables in Acceptables in	ragon V ragon APQ800 Q8053, APQ809 DM9206 MB905 SM8909 SM8939, SM8939, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953,	7oice & 9, 8, 5, 77, , W, CS605, M450, M710, 24, 8150,				
Improper Validation of Array Index	21-11-2019	4.6	Out-o occur to imp array Auto, Electr Snape Snape Snape Snape APQ8 APQ8 APQ8 MDM MDM MSM8 MSM8	f-bounds in came proper ver index in Snapdra ronics Co dragon Ce dragon M dragon W 009, APC 053, APC 098, MD 9207C, M 9640, MI 8905, MS 8909W, M 8920, MS	s access ra drive alidation Snapdr gon Coronsume dustria dobile, foice & Marable (28017, 28096A) M9206, M9206, M98937, MSM8937, MSM8937,	can r due n of agon nsumer ity, or IOT, I IOT, Usic, es in U, 17,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1076
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Da	te CVS	6	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			QCN7 SDM6 SDX2	8996AU, '605, SD. 530, SDM 0 ( <b>D : CVE</b> -	A660, SI 1636, SD	OM450, M660,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-201	2.1	Improvarial firms bound funct through Auto, Snape Snape Snape Snape APQ8 MSM8 QCA6 QCS4 SDM8	oper valible receivare cand accession while gh loop Snapdradragon Caragon Caragon Maragon Websel (1988) APC (1984)	dation for ved from lead to define WLAI enteration Snaper Consumer	or loop n out of N ng dragon mpute, er ity, er IOT, d IOT, U, 98, 15, 1845,	https:/ w.qual m.com pany/i ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1077
Out-of- bounds Read	21-11-201	19 4.6	in fas to im while from Snapo Snapo Snapo Snapo Snapo APQ8 MSM8	r over-ret message proper in process firmwardragon Adragon Caragon Caragon Maragon Webber 1996 AU, 26053, AP 18996 AU, 2605, QC	ge handling a me e in auto, consume onnective doubte, voice & MONTON MEMBER	er due idation essage er ity, er IOT, l IOT, Music in U, 98,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1078
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pul	blish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
				SDX2	60, SDM 0, SDX2 <sup>2</sup> <b>D : CVE</b> -	1	·				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-	-11-2019	7.2	from source that to potent buffer Snape Sn	tmap file any un-a e, there he bitma dially ca r overflo dragon C dragon C dragon C dragon C dragon I dragon I dragon V 016, AP 098, MD 3996AU, par, QCS4 55P, SC8 45, SDM 660, SDM 50, SM7 50, SM7 50, SXR	authenticis a possing can use stacew. in auto, compute connective consumendustria Mobile, Moice & MOMOSO, QCS 180X, S. 1670, SD 150, SM 1130, SX 1130, SX 1130, SX	cated sibility k  k  vity, er ity, l IOT, l	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
Out-of- bounds Read	21-	-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in				https://w.qualm.com/pany/jct-securifiletinsber-20	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 APQ8 MDM' MSM8 QCA6 QCA9 SDA6 SDM6	009, AP0 053, AP0 098, MD 9207C, M 9650, M3 3998, QC 574AU, G 379, QC 60, SDM 660, SDM 645, SDX	Q8096A M9206, MDM960 SM8996 A6174A QCA937 S405, QO 630, SD 1670, SD 20, SM6	07, AU, 7, CS605, M636, M710,				
Out-of- bounds Read	21-11-2019	10	while session messar un-information of Snapor Snapo	r over reparsing on manages if ne tended voltagon of the degraph of the graph of th	downlingement of tworks ralues in auto, ompute onsume adustria oT, Snapplagon Vagon APQ800 Q8053, APQ809 DM9607 DM9605 DM8900 DM800	nk OTA sends  r IOT, l IOT, odragon oice & 9, 8, 5, 40, 5, 40, 5, 40, 6, 17, 68, CS605, A660,	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- MSM8- 031219	/1081
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID : CVE-2019-2271  Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IOT, Snapdragon	Weakness	Publish Date	CVSS	[	Descriptio	n & CVE	ID	Pat	:ch	NCIIP	CID
allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,				SDM6 SDM7 SDX20 SM61 SM82 Snapd	36, SDM 10, SDM 0, SDX24 50, SM7 50, dragon_H	660, SD 845, SD 5, SDX55 150, SM High_Med R2130	M670, M850, , , 8150, d_2016				
Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9615, MDM9615, MDM9615, MDM9615, MDM9650, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8917, MSM8920, MSM8917, MSM893, MSM8917, MSM893, MSM8940, MSM8953, MSM8964U, MSM8953, MSM8964U, MSM8953, MSM8964U, MSM8964U, MSM8964U, MSM8964U, MSM8964U, MSM8964U, MSM8964U, MSM8964U, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	uthenticati	21-11-2019	10	allows NAS n result bypas Snapd Snapd Snapd Snapd Snapd Snapd Snapd Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA84 SDM6	s MODEN nessages into aut is of NAS dragon A dragon C dragon Ir dragon Ir dragon Ir dragon Ir dragon Ir solve, Snapdr ables in A 017, APO 096AU, A 9150, MI 9615, MI 9635M, I	M to acco s which of thenticated in auto, ompute, onsume adustria oT, Snap aragon V ragon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9625 MDM9625 MB9676, MSM891 SM8937, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDA 1660, SD	ept any can tion  for IOT, l IOT, dragon foice & 9, 8, 5, 7, 7, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10	w.qual m.com pany/j ct- securit lletins ber-20	lcom l/com produ ty/bu /octo	MSM8-	/1082
CV Scoring Scale (CVSS)         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9											

Weakness	Publish Date	cvss	1	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SM61 SM82 Snapo , SXR1	lragon_F L130, SX	150, SM High_Me R2130	8150, d_2016				
			CVE I	D : CVE-	2019-2	289				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 Snape , SXR1	lragon_F	ress range the System the System to the Syst	ge sDBG , vity, or IOT, l IOT, lusic, 09, , CS404, 215, M429, M630, M660, M845, d_2016	https:/w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1083
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute,				https://w.qual m.com pany/j	com /com	H-QUA- MSM8- 031219	/1084
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Snapo Mobil Music Wear; APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	dragon Coloragon Infragon Infr	ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9655 SM8909, MSM891 SM8937, SM8940, SM8976, MSM8937, SM8940, SM8976, MSM8910, SM8976, MSM8910, SM8976, MSM8937, SM8976, MSM8937, SM8940, SM8976, MSM8937, SM893	1 IOT, dragon foice & 9, 8, 5, 40, 5, 40, 65, 4660, M439, M632, M670, M850, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	securit lletins, ber-20 bulleti	octo 19-		
N/A	21-11-2019	7.2	copy for the to the Paran are from the environment of the Environment	e invokin from fd o secure l neters be om non s onment. Snapdra dragon C dragon I	or local buffer, eing popsecure in Snapengon Corfonnectives	ouffer oulated dragon mpute, vity, er IOT,	https://w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	/com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
nicobar					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, 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/october-2019-bulletin	H-QUA-NICO- 031219/1086

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM4 SDM6 SDM6 SDM6 SDM8 SDX58 SM81 Snapo	9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 9650, MS 3905, MS 3920, MS 3940, MS 3976, MS 3976, MS 3976, MS 3976, SDM 45, SDM 45, SDM 45, SDM 5, SM615 50, SM82 dragon_H	DM9607 DM9625 MDM9645 DM9655 SM8909, MSM891 SM8953, SM8953, SM8956, S605, Ql S605, SD S632, SD S670, SD	M215, A845, M450, M710, X20, 150,				
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack o will be modifi- stated bound Auto, Electr Snapo Snapo Mobil Music Weara	condition f resource e concur fied in the nent lead d access Snapdra conics Co dragon C dragon I dragon I fragon I frago	ce lock verently e memouslin Snapologon Coronsume onsume other Snapologon Veragon Veragon	which  py t of dragon asumer ity, r IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
			APQ8 MDM9 MDM9	017, APC 096AU, A 9206, MI 9607, MI 9650, MS	APQ809 DM9207 DM9640	'C, ),				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID: CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8933, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA645, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-NICO- 031219/1088

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10490		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-NICO- 031219/1089
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-NICO- 031219/1090

3-4

4-5

8-9

7-8

9-10

6-7

5-6

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Pu	blish Date	cvss		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
				APQ8 APQ8 MSM8 Nicob SA61 SDA8 SDM6 SDM6 SM61 SM82	dragon V 1016, AP 1098, MD 18996AU, 1996AU,	Q8096A M9205, MSM89 405, QCS 180X, SD 630, SD 1670, SD 1850, SD 150, SM	U, 98, 605, DA660, M636, M710, X24, 8150,				
Use After Free	21-	-11-2019	4.6	Possil kerne came: modu Snapo Snapo Snapo Mobil Music Wear Wired Netw IPQ40 MDM MSM8 QCA9 SDM8 SM81	ble doub el while la ra senso dles pow dragon de dragon la dragon	ole free is nandling r and its er seque nuto, consume ndustria oT, Snap dragon lapdrago ructure s n APQ80 8064, DM9207 SM8909 Nicobar, S405, Q0 24, SM7	ssue in the sub ence in IOT, dragon oice & on and 53,	https:/w.qualm.com pany/ct- securi lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- 031219	
Out-of- bounds Read	21-	-11-2019	10	while session messa un-in Snapo	r over re parsing on mana ages if no tended v dragon A	downlingement (etwork s values in	nk OTA sends	https://w.qualm.com pany/ct-securilletins	lcom 1/com produ ty/bu	H-QUA- 031219	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIII	PC ID
			Snapo Snapo Snapo Mobil Musio Wear: APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	dragon Caragon Indragon Indrag	onsume adustria oT, Snap tragon Vagon APQ800 Q8053, APQ809 DM9625 MDM9625 MDM9655 MB9676, MSM8937, SM8940, SM8976, ASM8976, ASM89	r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, 40, 5, M439, M632, M670, M850, 8150,	ber-20 bulleti	19-		
Improper Authenticati on	21-11-2019	10	allow NAS n result bypas Snapo Snapo Snapo Snapo	of integr s MODEI nessages into aut ss of NAS dragon A dragon C dragon I dragon I	M to accombined to accombine the strategy of t	ept any can tion , r IOT, l IOT,	https://w.qualm.com pany/pct-securit lletins/ber-20 bulleti	com /com orodu cy/bu /octo 19-	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch:	NCIIF	PC ID
			Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDA8 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	e, Snapdrables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 9635M, I 3905, MS 3905, MS 3905, MS 3905, MS 3953, MS 3	Tagon V ragon APQ800 Q8053, APQ809 DM9607 DM9625 MDM9655 MSM8937, MSM8940, MSM8940, MSM8940, MSM8940, MSM8956, MSM8940, SM8940, SM8955, MSM8940, MSM8955, MSM8940, MS	oice & 9, 8, 5, 7, 5, 40, 5, 7, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape	nation d k of addr done on dragon A dragon C dragon C dragon I dragon W dragon W	ress rang the Sys code. in uto, ompute onnectiv onsume ndustria Iobile, roice & M	ge DBG , vity, er IOT, l IOT,	https://w.qualm.com pany/jct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			APQ8 MDM9 MSM8 MSM8 MSM8 QCS40 SDA60 SDM6 SDM6 SDM6 SDM8 Snapo	dragon_F	Q8053, SM8905 SM8917, SM8937, SM8953, cobar, Q S05, QM2 S45, SDM S450, SD S636, SD S710, SD	CS404, 215, 4429, M630, M660, M845,				
				P modul						
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM MSM MSM MSM MSM	out side it receive its receive lessage. Snapdra dragon Id dragon	its bounces malforin Snapor Corronsume adustria oT, Snapor APQ800 Q8053, APQ809 DM9605 DM9605 DM9655 DM8965 DM8966	ndary ormed dragon npute, or IOT, l IOT, dragon oice & 9, 8, 6, 7, 7, 40, 6, 77,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	lcom n/com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)										

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, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID: CVE-2019-2303		
apq8053					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-APQ8- 031219/1096

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	tch	NCIIP	CID
			SDM6 SDM8 SDX5 SM81 Snapo , SXR1	30, SDM 60, SDM 45, SDM 5, SM615 50, SM83 dragon_F 130, SX <b>D : CVE</b> -	670, SD 850, SD 50, SM7 250, High_Me R2130 <b>2019-2</b>	M710, X20, 150, d_2016				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated to will be modifi	condition f resource f resource e concur fied in the nent lead d access Snapdra conics Co dragon In dragon	ce lock verently e memorals to out in Snaporals gon Corrective onsume industria oT, Snaporagon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905 MSM89	which  py t of dragon isumer ity, r IOT, dragon oice &  9,  8, 7C, 0, , 89, AU, CS605, 845, M630, M660, X20, 150,	https:/w.qualm.com pany/ct- securilletins ber-20 bulleti	lcom n/com produ ty/bu /octo	H-QUA- 031219	_
Use After	21-11-2019	2.1	Use at	fter free	issue in	Xtra	https:/	•	H-QUA-	_
Free			daem	on shutd	lown du	e to	w.qua	lcom	031219	/1098
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	ch	NCIIP	C ID
			static freed in Snape Snape Snape Snape Snape Snape Snape Mobil Music Wear: APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SM61 SM82	object in from a mapdragon Caragon Caragon Indragon Indra	astance genultiple in Auto, ompute, onnectivonsume industria oT, Snap aragon Vagon APQ800 APQ809 APQ	getting places  vity, r IOT, l IOT, dragon oice &  9, 8, 7, W, CS605, M710, 24, 8150,	m.com pany/s ct- securit lletins ber-20 bulleti	c/com produ ty/bu /octo		
Improper Validation of Array Index	21-11-2019	4.6	occur to imp array Auto, Electr Snapo Snapo Snapo Snapo Snapo APQ8	f-bounds in came proper value index in Snapdra conics Co dragon C dragon Ir dragon W dragon W 009, APC	ra drive alidation Snapdra gon Cor onsume ndustria Iobile, Toice & M Vearable Q8017,	r due n of agon nsumer ity, r IOT, l IOT, fusic, es in	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MDM MSM8 MSM8 MSM8 MSM8 QCN7 SDM6 SDX2	098, MD 9207C, M 9640, MS 3905, MS 3909W, I 3920, MS 3996AU, 605, SDA 630, SDM 0	MDM960 DM9650 SM8909, MSM891 SM8953, MSM89 A660, SI	98, 0M450, M660,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	varial firmw bound function through Auto, Snape Snape Snape APQ8 APQ8 MSM8 QCA6 QCS4 SDM8	oper valioner valioner validaccess on while gh loop is Snapdradragon Conics Codragon Indragon Miragon Miragon Williagon Miragon Williagon Miragon Williagon	ved from lead to o in WLAI e iteratin in Snapo agon Cor onsume onnectiv onsume dobile, oice & M Q8096A MSM89 QCN760 605, SDA	n out of N ng Iragon npute, r ity, r IOT, I IOT, U, 98, 5,	https:/ w.qual m.com pany/i ct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	·
Out-of- bounds Read	21-11-2019	4.6	in fast to imp while from Snapo Snapo	r over-re t messag proper in process firmwar dragon A dragon C	e handle nput vali ing a me e in auto, onsume	er due idation essage r	https://w.qualm.com pany/jct- securifiletins ber-20	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
				Snapo Snapo Snapo APQ8 MSM8 QCN7 SDA6 SDX2	dragon C dragon M dragon V 053, APC 8996AU, 605, QC 60, SDM 0, SDX24	ndustria Iobile, Ioice & N Q8096A MSM89 S405, Q0 636, SDI	d IOT, Music in U, 198, CS605, M660,	bulleti	n		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-	-11-2019	4.6	wlan rates elements than in Snape Snape Snape Snape APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	r overflomodule or extendent lengt max rate dragon of dr	if suppo ded rate h is grea set leng auto, compute consume onnectiv consume dobile, voice & N Q8053, MDM92 MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0 670, SDI 20, SM6	rted es ater gth in , er rity, er IOT, al IOT, Music in 06, 07, c, AU, CS605, M710, 150, R2130	https:/w.qualm.com pany/ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	-
Use After Free	21	-11-2019	4.6	kerne came modu	ble doub I while I ra senso Iles pow Iragon A	nandling r and its er seque	the sub	https://w.qual m.com pany/	com /com	H-QUA- 031219	•
CV Scoring Scal (CVSS)	е	0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch:	NCIIP	CID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID: CVE-2019-2266				securit lletins ber-20 bulleti	octo 19-		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- 031219	•
Out-of-	21-11-2019	10	Buffer over read can happen			https:/	//ww	H-QUA-	APQ8-	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	I	Descriptio	n & CVE	ID	Pat	ch	NCIIF	PC ID
bounds Read			while	parsing	downlir	ık	w.qual	com	031219	7/1105
			sessio	n manag	gement (	OTA	m.com	/com		
			messa	iges if ne	twork s	ends	pany/j	produ		
			un-int	ended v	alues in		ct-			
			*	lragon A	•		securit	ty/bu		
				lragon C			lletins			
			*	lragon C		•	ber-20			
			_	lragon Ir			bulleti	n		
			^	lragon Io	•	•				
				e, Snapd	•	oice &				
				, Snapdr	_	_				
				ables in A	-	9,				
			·	017, AP(	•	_				
			~	096AU, A	•	•				
				9150, MI						
				9206, MI						
				9615, MI						
				9635M, I						
				9650, MI		•				
				8905, MS	•					
				8909W, N		•				
				3920, MS						
				8939, MS 8953, MS						
				3933, M3 3996AU,						
				ar, QCM:		•				
				.5, SC818	. •	-				
			-	45, SDM						
				50, SDM	•	•				
				36, SDM	•	•				
				10, SDM	•	•				
				10, SDX24	•	•				
				50, SM7:	•	•				
			SM82		150, 5141	0150,				
				lragon_H	ligh Me	d 2016				
			_	.130, SXI	Ū	u_2010				
				D : CVE-		271				
Improver			Lack o	of integri	ty checl	K	https:/	//ww		
Improper Authenticati	21-11-2019	10		s MODEN	•		w.qual	•	H-QUA-	APQ8-
	21-11-2019	10	NAS messages which can				m.com/com		031219/1106	
on			result into authentication				pany/j	•		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
			٠.	s of NAS			ct-			
			•	lragon A	•		securi			
			•	lragon C	•		lletins			
			_	lragon C			ber-20			
			•	lragon Ir			bulleti	n		
				lragon Io						
				e, Snapd	•	oice &				
				, Snapdr	_	0				
				ables in A	-	9,				
			•	017, APO 096AU, A	•	0				
			•	9150, MI	•					
				9130, MI 9206, MI						
				9615, MI		•				
				9635M, I						
				9650, MI		•				
				3905, MS						
				3909W, I	•					
				3920, MS						
				3939, MS	•					
				3953, MS						
				3996AU,						
			Nicob	ar, QCM	2150, Q	CS605,				
			QM21	.5, SC818	30X, SD <i>A</i>	1660,				
			SDA8	45, SDM	429, SDI	M439,				
			SDM4	50, SDM	630, SD	M632,				
			SDM6	36, SDM	660, SD	M670,				
			SDM7	10, SDM	845, SD	M850,				
			SDX2	0, SDX24	, SDX55	,				
			SM61	50, SM7	150, SM	8150,				
			SM82	•						
			Snapo	lragon_F	ligh_Me	d_2016				
			, SXR1	[130, SX]	R2130					
			CVE I	D : CVE-	2019-2	289				
Improper			Inform	nation d	isclosur	e due	https:/	//ww		
Restriction			to lac	k of addr	ess rang	ge	w.qual	com		
of			check	done on	the Sys	DBG	m.com	/com	H-QUA-	AP08-
Operations	21-11-2019	2.1	buffer	rs in SDI	code. in		pany/produ		031219	-
within the			_	lragon A			ct-			, ===,
Bounds of a			Snapdragon Compute,				securi			
Memory			Snapdragon Connectivity,				lletins	/octo		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
Buffer			Snapo Snapo Snapo Infras Netwo APQ8 MDM' MSM8 MSM8 MSM8 QCS40 SDM6 SDM6 SDM6 SDM6 SDM8 Snapo , SXR1	lragon_H 130	ndustria Mobile, Joice & Mobile Vired and APQ80 Q8053, SM8905 SM8917, SM8937, SM8953, SM895	l IOT, fusic, 09, , CS404, 215, M429, M630, M660, M845, d_2016	ber-20 bulleti			
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing non- standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			QCA6 QCA9 QCS4 SDA8 SDM8 SM81	3996AU, 574AU, ( 379, QCI 05, QCS6 45, SDM 345, SDX 50 <b>D : CVE</b> -	QCA937 N7605, 05, SDA 636, SDI 20, SDX <b>2019-2</b>	7, 4660, M660, 24, <b>297</b>				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	out side it receive sessage. It receives sage. It sages of the sages o	its bountes malformatics malformatics malformatics on consume adustria of the consume of the consumer	ndary ormed dragon inpute, er IOT, il IOT, idragon oice & 19, 15, 17, 17, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			•	dragon_F 1130, SX	Ū	d_2016				
			CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	copy for the Paramare from the Paramare Snape Sn	e invoking from fd of a secure laneters be om non somment. Snapdradragon Caragon Maragon Waragon Maragon Maragon Maragon Maragon Maragon Maragon Maragon, Maragon, Maragon, Maragon, Maragon, Maragon, Maragon, Maragon, Maragon, SDA Go, SDA	or local laborator local laborator, eing poper secure in Snaper agon Corronsume adustria dobile, foice & More and a APQ80 (28053, Q8096A (28053, Q805, Q8	ouffer oulated dragon inpute, vity, or IOT, I IOT,	https:/w.qualm.com pany/jct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	-
Out-of-	21-11-2019	2.1	Non Secure Kernel can cause				https://ww		H-QUA-	•
bounds Read			Trust	zone to d	do an ar	bitrary	w.qual	com	031219	/1111
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318	m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	
mdm9207c					
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, 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/october-2019-bulletin	H-QUA- MDM9- 031219/1112

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150		
			CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/1113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130		
			CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8909, MSM8909W, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM896AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/1114
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/1115
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	sh Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
				APQ8 MDM' MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	017, APC 096AU, 9207C, M 9650, M 3996AU, 174A, Q 377, QC 605, QC 45, SDM 45, SDM 50, SM8	MDM92 MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0 670, SD1 20, SM6 250, SXI	07, , , AU, CS605, M710, 150, R2130				
Use After Free	21-11	1-2019	4.6	CVE ID: CVE-2019-10566  Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150				https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- MDM9- 031219	/1116
Out-of- bounds Read	21-11	1-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,				https://w.qualm.com pany/j ct- securit lletins	lcom l/com produ ty/bu	H-QUA- MDM9- 031219	/1117
CV Scoring Scal (CVSS)			6-7	7-8	8-9	9-10					

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo APQ8 APQ8 MDM <sup>o</sup> MSM8 QCA6 QCA9 SDA6 SDM8	dragon C dragon I dragon V dragon V 009, APO 053, APO 098, MD 9207C, M 9650, M 9650, M 379, QC 379, QC 60, SDM 660, SDM	ndustria Mobile, Moice & M Q8017, Q8096A MM9206, MDM960 SM8996 CA6174A QCA937 S405, QO 630, SD 1670, SD	U,  O7, AU, CS605, M636, M710, 150	ber-20 bulleti			
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electric Snape Sn	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660,				//ww lcom produ ty/bu /octo 019- n	H-QUA- MDM9- 031219	/1118
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150		
			CVE ID : CVE-2019-2297		
msm8905					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MSM8- 031219/1119

Weakness	Publish Date	cvss	[	Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack o will be modificated bound Auto, Electric Snaped Snaped Snaped Mobil Music Wears APQ8 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 SDM6 SDM7 SDX24 SM81		ce lock werently e memorish shape in Snape in Snape in Snape industria oT, Snape ragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905 MSM80	which rpy t of dragon nsumer ity, r IOT, l IOT, dragon oice & 19, 8, 7C, 0, , 89, AU, CS605, 845, M660, X20, 150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Wear APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SM82	c, Snapdr ables in 2 017, APC 096AU, 2 9150, MS 9207C, MS 39650, MS 3917, MS 3940, MS 3996, MS 3996, MS 3998, Nic 60, SDAS 50, SDAS 50, SM7	APQ800 Q8053, APQ809 DM9206 MDM960 SM8905 SM8909 SM8939, SM8939, SM8953, SM8953, SM8953, SM8953, SM8953, SM8958, SM8958, SM8958,	8, 5, 77, , W, AU, CS605, M450, M710, 24, 8150,				
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM896AU, MSM8998, QCN7605, SDA660, SDM450,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1122
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	tch	NCIIP	CID
			SDM6 SDX2	30, SDM 0	1636, SD	M660,				
			CVE I	D : CVE-	2019-1	0503				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	wlan rates elementhan in Snapor Snapor Snapor Snapor Snapor Snapor Snapor APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 QCN7 SDA8 SDM8	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130				//ww lcom n/com produ ty/bu /octo )19- n	H-QUA- MSM8- 031219	
				D : CVE-						
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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:/ w.qual m.com pany/ct- securi lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Wearables in APQ8009, APQ8017, APQ8003, APQ8017, APQ8003, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9650, MDM9655, MSM8909, MSM8905, MSM8909, MSM8909, MSM89037, MSM890, MSM8937, MSM8933, MSM8940, MSM8933, MSM8940, MSM8933, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8958, Nicobar, QCM215, QCS605, QM215, SC8180X, SDA660, SDA845, SDM430, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SKR1130, SKR2130	Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Uoice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,  allows MODEM to accept any NAS messages which can result into authentication https://www.qualcom m.com/com pany/produ ct-security/bu lletins/octo ber-2019-bulletin				APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	017, APC 096AU, A 9150, MI 9206, MI 9635M, I 9635M, I 9650, MS 8905, MS 8909W, I 8920, MS 8939, MS 8953, MS 8953, MS 8953, MS 8953, MS 8953, MS 8953, MS 805, SDM 10, SDM 10, SDM 10, SDM 10, SDM 10, SDM 110, SDM 110, SDM 110, SM7 110, SM7	Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 SM8909, MSM8910, SM8937, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDA 1630, SDA 1630, SDA 150, SM High_Me R2130	8, 5, 7, 6, 40, 5, 40, 5, 7, 98, CS605, A660, M439, M670, M850, 6, 8150,				
	Authenticati	21-11-2019	10	allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,				w.qual m.com pany/i ct- securit lletins ber-20	com /com produ ty/bu /octo	MSM8-	/1125
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	_	e 0-1	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM8953, MSM8976, MSM8953, MSM8976, SDM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape Snape Snape Snape Snape Snape Snape Snape Snape Month MSM8	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937,			https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1126
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 QCS44 SDA6 SDM4 SDM6 SDM6 SDM8 Snapo	dragon_F	cobar, Q 605, QM 845, SDN 4450, SD 636, SD 710, SD	CS404, 215, M429, M630, M660, M845, d_2016				
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electric Snapo Sn	r overflooprocess, and NAN space, in Snapdra conics Codragon Indragon Varagon Varagon, APO 19, IPQS 9206, MI 9607, MI 9650, MI	ing non- message Snapdra gon Cor onsume dustria fobile, foice & M Vired and APQ80 Q8053, Q8096A B064, IP DM9640 SM8905 QCA617 QCA937 N7605, 605, SDA 636, SDA	ge from agon sumer ity, er IOT, l IOT, l IOT, Q8074, 7C, 0, 74A, 7, 4660, M660, 24,	https:/w.qualm.com pany/ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1127
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary				https:/ w.qual	•	H-QUA- MSM8-	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Descriptio	n & CVE	ID	Pat	ch	NCIIF	PC ID
			when	it receiv	es malfo	ormed	m.com	/com	031219	/1128
			XID m	essage. i	n Snapo	lragon	pany/j	produ		
			Auto,	Snapdra	gon Con	npute,	ct-			
			•	lragon C			securit			
			•	lragon Ir			lletins			
			•	lragon Io		O	ber-20			
				e, Snapd	•	oice &	bulleti	n		
				, Snapdr	_	0				
				ables in A	_	9,				
			_	017, AP(	•	O				
			•	096AU, <i>I</i> 9150, MI	•					
				9206, MI						
				9615, MI		•				
				9635M, I		•				
				9650, MI		•				
				3905, MS						
				3909W, N						
			MSM8	3939, MS	M8940,					
			MSM8	3953, MS	M8976,					
			MSM8	3996AU,	MSM89	98,				
			Nicob	ar, QCM	2150, Q	CS605,				
			-	5, SC818						
				45, SDM						
				50, SDM	,	•				
				36, SDM	•	•				
				10, SDM	•	•				
				), SDX24	•	•				
				50, SM7	150, SM	8150,				
			SM82	-	liah Ma	J 2016				
				lragon_H .130, SXI		u_2016				
			CVE I	D : CVE-	2019-2	303				
				invokin	_		https:/	•		
				rom fd c		ouffer	w.qual		11 0114	
NI / A	21 11 2010	7.2	to the secure buffer, Parameters being populated				m.com/com		H-QUA-	•
N/A	21-11-2019	7.2				ulated			MSM8-	/1120
			are from non secure environment. in Snapdragon					ct-		/1129
					-	_	securit			
CV Scaring Seel			Auto,	Snapdra	gon con	npute,	lletins	OCTO		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			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, MSM8917, MSM8940, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315	ber-2019- bulletin	
qcn7605					
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCN7- 031219/1130
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			Music Wears APQ8 APQ8 MDM' MDM' MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7	e, Snapdr c, Snapdr ables in A 017, APC 096AU, A 9206, MI 9650, MI 39650, MI 3998, Nic 605, QCS 5, SDA6 29, SDM 110, SDM 4, SM615	ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8936 cobar, S405, Q0 6439, SD 636, SD	9, 8, 7C, ), , 89, AU, CS605, 845, M630, M660, X20,				
			Out-o occur to imp	D: CVE- f-bounds in came proper voindex in Snapdra	s access ra drive alidation Snapdr	can r due n of agon				
Improper Validation of Array Index	21-11-2019	4.6	Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8940, MSM8953, MSM896AU, MSM8998, QCN7605, SDA660, SDM450,				https://w.qualm.com pany//ct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20  CVE ID: CVE-2019-10535	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCN7- 031219/1132
Out-of- bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8996AU, MSM8996AU, MSM8996, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCN7- 031219/1133
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCN7- 031219/1134
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing non- standard NAN message from user space. in Snapdragon Auto, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QCN7- 031219/1135

9-10

CV Scoring Scale

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297		
sdm845					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM8- 031219/1136

Weakness	Pu	blish Date	CVSS	Description & CVE ID					ch	NCIIP	C ID
				SDM4 SDM6 SDM6 SDM5 SDX5 SM81 Snapo	30X, SDA 29, SDM 30, SDM 660, SDM 5, SM61 50, SM8 dragon_H 1130, SX <b>D: CVE</b> -	1439, SD 1632, SD 1670, SD 1850, SD 50, SM7 250, High_Me R2130	M450, M636, M710, X20, 150, d_2016				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-	-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130				https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	
Time-of- check Time- of-use (TOCTOU) Race Condition	21-	-11-2019	4.4	lack of will be modified stater bound Auto, Electron Snapo	condition of resour e concur fied in the ment lead access Snapdra conics Collragon Idragon Idr	ce lock werently de memods to out in Snaperson Coronnective consumendustria	which rpy t of dragon nsumer ity, r IOT,	https:/ w.qual m.com pany/ct- securi lletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			Music Wears APQ8 APQ8 MDM' MDM' MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7	e, Snapdrables in A 017, APC 096AU, A 9206, MI 9607, MI 9650, MS 3909W, M 3953, MS 3998, Nic 605, QCS 29, SDM 4, SM615 50	ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8996, cobar, S405, Q0 6439, SD 636, SD	9, 8, 7C, 9, 89, AU, ES605, 845, M630, M660, X20,				
Use After Free	21-11-2019	2.1	Use and daem static freed in Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MSM8 MSM8 MSM8	D: CVE- fter free from shutd object in from a m pdragon C dragon C dragon Ir	issue in lown du stance plustiple in Auto, ompute onsume onsume onsume ragon Vagon APQ800 Q8053, APQ809 QM9206 GM8905 GM8909 GM8909 QM8939, GM8939, GM	Xtra e to getting places vity, r IOT, l IOT, dragon oice & 9, 8, 7, W,	https:/ w.qual m.com pany/j ct- securif lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID				Pat	ch	NCIIP	C ID
			MSM8 SDA6 SDM6 SDM8 SM61	3996, MS 3998, Ni 60, SDA 660, SDM 45, SDX 50, SM7	cobar, Q 345, SDN 1670, SD 20, SDX 150, SM	CS605, M450, M710, 24,				
			CVE I	D : CVE-	2019-1	0490				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8996AU, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
				D : CVE-						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6			5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 APQ8 MDM' MSM8 QCA6 QCA9 QCN7 SDA8 SDM8	dragon V 017, APO 096AU, 1 9207C, M 9650, M 9996AU, 174A, QO 377, QC 605, QC 45, SDM 45, SDX 50, SM8	Q8053, MDM92 MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0 670, SD 20, SM6 250, SXI	06, 07, c, AU, CS605, M710, 150, R2130				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bi from a source that the potent buffer Snape Sna	tmap file any un-a e, there he bitma tially car roverflo dragon C dragon C dragon C dragon In dragon In dragon W 016, APO 098, MD 3996AU, ar, QCS4 55P, SC8 45, SDM 60, SDM 50, SM7 50, SM7 50, SXR2	e is load authentics a possup can use staction with the connection on sume adustrial lobile, loice & Month of the consumer of	ed cated sibility k  vity, er city, er IOT, d IOT, Music in U, 98, 6605, DA660, M636, M710, X24, 8150, XR2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Use After	21-11-2019	4.6	Possible double free issue in			https:/	//ww	H-QUA-	SDM8-	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
Free			camer modu Snapo Snapo Snapo Mobil Musio Wears Wired Netwo IPQ40 MDM0 MDM0 MSM8 QCA9	l while he a sensor les power lagon Aragon Icagon I	r and its er seque uto, onsume dustria oT, Snap ragon vagon apdrago APQ80 3064, OM9207 SM8909 Vicobar, S405, Q0	ence in er IOT, el IOT, edragon oice & on and e53, e7C, e7C,	w.qual m.com pany/j ct- securit lletins ber-20 bulleti	/com produ ty/bu /octo	031219	/1143
				D : CVE-						
Out-of- bounds Read	21-11-2019	7.5	P2P a handl mana, Snapo Snapo Snapo Snapo APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 SDA6	ole OOB action fra ing WLA gement for agon A dragon Conics	mes when Norame in uto, onsume industria lobile, oice & Marco Marc	ile  ir ity, ir IOT, il IOT, lusic in U, A, 7, CS605, M636,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-3	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150		
			CVE ID : CVE-2019-2268		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8937, MSM8937, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8- 031219/1145
CV Scoring Scal	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

(CVSS)

Lack of integrity check   allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon of Nobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8098, MDM9205, MDM9205, MDM9205, MDM9607, MDM9615, MDM9625, MDM9650, MDM9650, MDM9650, MDM9650, MDM9650, MDM9650, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8937, MSM8939, MSM8940, MSM8933, MSM8940, MSM8933, MSM8940, MSM8933, MSM8940, MSM8933, MSM8940, MSM8933, MSM8940, MSM8933, MSM8940, MSM8935, SDM630,	Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Restriction of 21-11-2019 2.1 to lack of address range check done on the SysDBG m.com/com 031219/1147	Authenticati	21-11-2019	10	allowing NAS in result bypas Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM's MDM's MDM's MDM's MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	s MODEN nessages into aut s of NAS lragon A lragon C lragon In lra	M to acc swhich of thentical in uto, ompute onsume industrial oT, Snap ragon V agon APQ800 Q8053, APQ809 DM9605 DM9625 DM9625 DM9625 DM9625 DM9635 SM8909, MSM891 SM8937, SM8940, SM8976, MSM891 SM891	ept any can tion  for IOT, al IOT, adragon foice & foi	w.qual m.com pany/j ct- securit lletins ber-20	com /com orodu cy/bu /octo	_	
of check done on the SysDBG m.com/com	Restriction	21-11-2019	2.1	to lack of address range				w.qualcom			
	of  CV Scoring Scal	e 0-1	1-2	check done on the SysDBG  2-3 3-4 4-5 5-6				m.com	/com 7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Operations within the Bounds of a Memory Buffer			buffer Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM6 SDM8 Snapo	rs in SDI dragon A dragon C dragon C dragon I dragon W dragon V dragon V dragon V dragon V dragon W 39205, MS 3940, MS 3	code. in auto, compute connective consume ndustria dobile, voice & March	cs404, cs404, dusic, Masic, Masic, Masic, Masic, Masic, Masic, Masic, Masic, Masic, Masic,	pany/j ct- securit lletins ber-20 bulleti	produ ty/bu /octo 119-		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stands user s Auto, Electr Snape Snape Snape Snape Snape Snape APQ8	r overflo process ard NAN space. in Snapdra conics Co dragon I dragon I dragon V dragon V dragon V dragon V	ing non- I message Snapdra I message Snapdra I message Sonnective Sonsume I consume I dobile, I oice & M Vired E and I APQ80 Q8053,	ge from agon asumer ity, r IOT, l IOT, fusic,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>o</sup> MDM <sup>o</sup> MSM8 QCA6 QCA9 QCS4 <sup>o</sup> SDA8 SDM8 SM81	019, IPQ8 9206, MI 9607, MI 9650, MS 3996AU, 574AU, ( 379, QCS 05, QCS6 45, SDM 845, SDX 50 <b>D: CVE</b> -	DM9207 DM9640 GM8905 QCA617 QCA937 N7605, 05, SDA 636, SDI 20, SDX2	7C, , , 74A, 77, .660, M660, 24,				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	P modul out side it received sage. it sage. it sage it	its bour es malfo in Snapo gon Cor onsume idustria oT, Snap ragon APQ800 Q8053, APQ809 OM9605 OM9605 OM9625 MB9607, MSM891 M8937, MSM891 MSM8940,	ndary ormed dragon npute, r IOT, dragon oice &  9,  8,  6,  7,  40,  6,  47,  48,  CS605, A660, M439, M632,	https:/w.qualm.com pany/jct-securifiletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-9	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8- 031219/1150

Weakness	Publish Date	CVSS	Descrip	tion & CVE	ID	Pat	ch	NCIIP	CID
			, SXR1130,	SXR2130					
			CVE ID : CV	E-2019-2	315				
Use After Free	21-11-2019	7.2	Use after from cleanup round missing point of a failed application. Compute, S. Consumer I. Industrial I. Mobile, Snat Infrastructu. Networking QCS404, QCSDM670, SISDX55, SM6SM8150, SX	nter saniti start of a train Snapdr napdragor OT, Snapdr pdragon V are and g in MDM9 (S605, SDA (DM710, SD (S150, SM7	zation rusted ragon ragon Vired 205, 845, M845, 150,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-S 031219,	
apq8017			CVE ID : CV	E-2019-2	349				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While proce Reject mess condition is resulting in in Snapdragor Snapdragor Snapdragor Snapdragor Mobile, Snap Wearables is APQ8017, A APQ8096AI MDM9150, MDM9615, MDM9635N MDM9650, MSM8905, MSM8909V	rage, Valid not met to an infin gon Auto, a Compute a Consume a Industria a IoT, Snap pdragon V dragon an APQ800 APQ8053, J, APQ809 MDM9607 MDM9607 MDM9605 MDM9605 MDM9655 MSM8909	exit ite loop  r IOT, l IOT, dragon oice &  9,  8, 5, 7, 6, 40, 5,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-A 031219,	•
CV Scoring Scal	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID				Pat	ch	NCIIP	C ID
			MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	3920, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDM 30, SDM 345, SDM 50, SM8 4130, SX	5M8953 5M8996 cobar, S605, Q 6660, SD 1439, SD 1632, SD 1670, SD 1850, SM7 250, High_Me	M215, 0A845, 0M450, 0M636, 0M710, 0X20,				
			CVE I	D : CVE-	2019-2	335				
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated and modificated an	condition of resour econcurried in the ment lead access Snapdragon Idragon Idr	ce lock werently the memory ds to out in Snape the gon Core consume the dustrial oT, Snape tragon V ragon APQ800 Q8053, APQ809 DM9640 SM8905 MSM8935 Cobar, S405, Q0 60, SDA	which rpy t of dragon nsumer rity, r IOT, dragon roice & roice & roice,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	_
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150		
			CVE ID: CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130  CVE ID: CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8- 031219/1154
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://ww w.qualcom m.com/com pany/produ ct- security/bu	H-QUA-APQ8- 031219/1155
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM <sup>o</sup> MSM8 MSM8 MSM8 MSM8 MSM8	dragon C dragon In dragon V dragon V dragon W 009, APC 053, APC 098, MD 9207C, M 9640, MS 3905, MS 3905, MS 3905, MS 3905, MS 3905, SDA 30, SDM	ndustria Jobile, Joice & M Vearable Q8017, Q8096A M9206, MDM960 DM9650 DM9650 MSM8937, MSM8933, MSM89	I IOT,  Music, es in  U,  77, 7, 17, 18, 198, 0M450,	lletins ber-20 bulleti	19-		
			Buffer	D : CVE-	w can o	ccur in				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	rates elementhan rates from than rates from the Snape of	module i or extendent length nax rate dragon A dragon C dragon Indragon Ind	ded rate h is grea set leng uto, ompute onsume onsume onsume dustria lobile, loice & M Q8053, MDM92 MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0	es ater gth in , er ity, er IOT, l IOT, fusic in 06, 07, , AU, CS605,	https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			SM81	345, SDX 50, SM8 <b>D : CVE</b> -	250, SXI	R2130				
Out-of- bounds Read	21-11-2019	7.5	P2P a handl mana Snapo Snapo Snapo Snapo APQ8 APQ8 MDM MSM8 QCA6 QCA9 SDA6 SDM8	ble OOB ction fra ling WLA gement dragon A dragon C dragon I dragon I dragon V 009, AP 053, AP 098, MD 9207C, M 9650, M 574AU, 379, QC 60, SDM 660, SDM 645, SDX D: CVE-	ames whan Inframe in Auto, Consume Industria Mobile, Voice & M Q8017, Q8096A MM9206, MDM960 SM8996 CA6174A QCA937 S405, QC 630, SD 1670, SD 20, SM6	ile  r ity, r IOT, l IOT, Music in  U, 7, AU, 7, CS605, M636, M710, 150	https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
Out-of- bounds Read	21-11-2019	10	while session messa un-in Snapo Snapo Snapo Snapo Mobil Musio Wear	r over reparsing parsing ages if no dragon Adragon Idragon Idr	downlingement of the setwork so walues in the setwork so walues in the setwork so walues was and ustriate of the setwork so walues was and walues wal	nk OTA sends or IOT, I IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch.	NCIIP	CID
			MDMMMDMMMDMMMDMMMSMMSMMSMMSMMSMMSMMSMMSM	096AU, A 9150, MI 9206, MI 9635M, II 9635M, II 9635M, II 8905, MS 8905, MS 8920, MS 8939, MS 8939, MS 8953, MS 8953, MS 8050, SDM 10, SDM 10, SDM 10, SDM 10, SDM 110, SDM 1110, SM 11110, SM 11110, SM	DM9205 DM9607 DM9625 MDM9645 SM8909, MSM891 SM8937, SM8940, SM8976, MSM89 2150, Q0 80X, SDA 429, SDA 1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	98, CS605, A660, M439, M632, M670, M850, ,				
Improper Authenticati on	21-11-2019	10	allown NAS named Snaped Snaped Snaped Snaped Mobil Musica Weard APQ8 APQ8 MDM	of integres MODEI nessages into aut s of NAS dragon A dragon C dragon I dragon I dragon I 017, APO 096AU, A 9150, MI	M to accombined	ept any can tion  r IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			MDM <sup>o</sup> MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	9615, MI 9635M, I 9650, MI 8905, MS 8909W, I 8920, MS 8939, MS 8953, MS 8953, MS 8953, MS 8953, MS 80, SDM 10, SDM 10, SDM 10, SDM 10, SDM 10, SDM 10, SDM 110, SM7 1130, SX D: CVE-	MDM96-55 M8909, MSM891 SM8940, SM8940, SM8976, MSM89 2150, Qu 80X, SDA 429, SDI 1630, SD 1660, SD 1845, SD 150, SM High_Me R2130	98, CS605, A660, M439, M670, M850, ,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information lack check buffer Snape	mation d k of addi done or s in SDI dragon C dragon C dragon I dragon W dragon W dragon W dragon W dragon W 39205, MS 3920, MS 3940, MS	isclosures range the System on the system of	e due ge DBG vity, r IOT, l IOT, fusic,	https:/w.qualm.com pany/jct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	_
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pub	lish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
				SDA6 SDM6 SDM6 SDM6 SDM8 Snapo	dragon_I	345, SDN 1450, SD 1636, SD 1710, SD High_Me	M429, M630, M660, M845, d_2016				
Integer Underflow (Wrap or Wraparound )	21-1	11-2019	4.6	while stand user's Auto, Electric Snape Snape Snape Infras Network APQ8 APQ8 IPQ40 MDM MDM MDM MSM8 QCA6 QCA9 QCS4 SDA8 SDM8 SM81	r overfloor process and NAN space. in Snapdra conics Coloragon Maragon Waragon Waragon, Maragon Waragon Waragon Waragon Waragon Waragon Waragon, Maragon Waragon, Maragon Waragon, Maragon Waragon, Maragon Waragon, Waragon W	ing non- I message Snapdra agon Cor connective consume ndustria Mobile, Vired e and n APQ80 Q8053, Q8096A 8064, IP DM9640 SM8905 QCA617 QCA937 N7605, 605, SDA 636, SDA	Je from agon agon sumer rity, er IOT, lot, lot, lot, lot, lot, lot, lot, lot	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com orodu cy/bu /octo 19-	H-QUA- 031219	•
Out-of- bounds Read	21-1	11-2019	7.5	array when	P modul out side it receiv nessage.	its bour es malfo	ndary ormed	https:/ w.qual m.com pany/	com /com	H-QUA- 031219	-
CV Scoring Scale (CVSS)	е	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	[	Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapd Snapd Snapd Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapd	Snapdra Iragon C Iragon In Iragon Ic e, Snapdra Snapdr	onsume industria of, Snap ragon Vagon APQ800 DM9605 DM9605 DM9605 DM9655 BM8909, MSM891 BM8937, SM8940, SM8940, SM8940, SM8956, SD E660, S	r IOT, l IOT, dragon oice & 9, 8, 40, 5, 7, 7, 28, CS605, M439, M670, M632, M670, M850, ,	ct- securit lletins, ber-20 bulleti	octo 19-		
N/A	21-11-2019	7.2	copy for to the Param are from envirous Auto,	invoking from fd of secure lands because the secure lands because the secure lands and secure lands are lands and secure land	or local bouffer, eing pop secure in Snapo gon Cor onnectiv	ouffer oulated dragon npute, vity,	https://w.qual m.com pany/j ct- securit lletins/ ber-20	com /com produ ty/bu /octo	H-QUA- 031219	-
CV Scoring Scal	e 0-1	1-2		<u> </u>		5-6				

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo Snapo Infras Netwo APQ8 APQ8 APQ8 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SM81 Snapo	dragon Indragon Wilragon Wilragon Wilragon Wilragon Wilragon Wilragon Wilragon Wilragon, APO (19205, MI) (19205, MI) (19305, SDA) (19305, SDA	ndustria Mobile, Vired and APQ80 Q8053, Q8096A M9150, DM9206 SM8920, SM8940, SM8940, SM8940, SM896, MSM89 MSM896, MSM8	1 IOT, flusic, 09, U, 98, 215, M429, M630, M660, M845, 7150, d_2016	bulleti			
Out-of- bounds Read	21-11-2019	2.1	Trust: memore result Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo APQ8	decure Ko zone to o ory read dragon A dragon C dragon I dragon V dragon V dragon V dragon V dragon V dragon V dragon V	do an ard which well in uto, connective consume ndustria Mobile, Voice & M Vired e and n APQ80 Q8096,	vity, r IOT, l IOT, fusic,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	-
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
on a 2000 con			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318		
apq8096au	T				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8933, MSM8976, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-APQ8- 031219/1165

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SM81 Snapo	5, SM61! 50, SM8 lragon_F l130, SX	250, ligh_Me					
			CVE I	D : CVE-	2019-2	335				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack of will be modificated bound Auto, Electron Snape Snape Mobil Music Wears APQ8 MDM MDM MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX2 SM81	condition f resour fe concur fied in the ment lead d access Snapdra conics Col dragon In dragon	ce lock werently the memorals to our in Snape ingon Corronnective onsume industria oT, Snape lragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM8905	which  py t of dragon nsumer ity, or IOT, l IOT, dragon oice &  9,  8, 7C, 0, , 89, AU, CS605, 845, M630, M660, X20, 150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
Use After Free	21-11-2019	2.1	Use at daem static freed	fter free on shute object in from a ranged	issue in lown du istance ; nultiple	Xtra e to getting	~ <sub> </sub> ,		H-QUA 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SM61 SM82	dragon Colragon Colragon Colragon Indicated In Indicated	connective on sume and ustrial off, Snap bragon APQ800 Q8053, APQ809 DM960 SM8905 SM8905 SM8939, SM8953, SM8956, SM895	vity, or IOT, ol IOT, odragon oice & 9, 8, 5, 77, , W, CS605, M450, M710, 24, 8150,	securit lletins ber-20 bulleti	/octo 119-		
Improper Validation of Array Index	21-11-2019	4.6	occur to imparray Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM	f-bounds in came proper v index in Snapdra conics Co dragon Idragon V dragon V 009, APO 053, APO 098, MD 9207C, M	ra drive alidation Snapdr Igon Cor Innectiv Ionsume Industria Mobile, Yoice & M Vearable Q8017, Q8096A M9206, MDM960	r due n of agon nsumer ity, er IOT, I IOT, Usic, es in U,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 QCN7	3905, MS 3909W, I 3920, MS 3940, MS 3996AU, 605, SDA 30, SDM	MSM891 SM8937, SM8953, MSM89 A660, SI	.7, 98, 0M450,				
			CVE I	D : CVE-	2019-1	0503				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	varial firmw bound functi throu Auto, Snapo Snapo Snapo APQ8 APQ8 MSM8 QCA6 QCS44 SDM8	oper valiole receivare can di accession while gh loop is Snapdradragon Chagon Chagon Maragon Wobsa, APO 1998, MD 1996AU, 1996A	ved from lead to of in WLAI e iteration in Snapo agon Cor consume consume donnective donsume ndustria MOSM89 Q8096A MSM89 QCN760 505, SDA 20	n out of N ng Iragon npute, r ity, r IOT, I IOT, U, 98, 5,	https:/w.qualm.com pany/ct- securilletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- 031219	•
Out-of- bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,				https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 MSM8 QCN7 SDA6	dragon V 053, AP0 3996AU, 605, QC 60, SDM 0, SDX24	Q8096A MSM89 S405, Q0 636, SDI	U, 98, CS605,				
			CVE I	D : CVE-	2019-1	0563				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	wlan rates element than rates of than rates of the strain	r overflomodule in extendent length max rate dragon Aragon Chragon Chragon Maragon Wolfragon Wol	if suppoded rate has greated set lenguto, compute consume ndustria Mobile, Momento Mobile, Momento Mobile, Momento Mobile, Momento Mom	rted es eter eth in r ity, r IOT, l IOT, fusic in 06, 07, , 7, AU, CS605, M710, 150, R2130	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	-
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute,				https://w.qualm.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	H-QUA- 031219	_
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	bulletin	
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8- 031219/1173

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

3-4

Weakness	Publish Date	cvss		Description & CVE ID		Pat	ch	NCIIP	C ID	
			CVE I	D : CVE-	2019-2	268				
Out-of- bounds Read	21-11-2019	10	while session messar un-information Snaped Snaped Snaped Mobil Music Wear APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	r over reparsing on manages if no tended version of the property of the proper	downlingement etwork stalues in auto, compute consume ndustria oT, Snap lragon Vagon APQ800 DM9625 DM9625 DM9625 DM9625 DM9655 SM8909 MSM8937 GM8937	nk OTA sends , er IOT, dl IOT, dragon oice & 19, 18, 5, 40, 5, 17, 17, 18, 18, 18, 18, 19, 18, 18, 19, 19, 10, 10, 10, 10, 10, 10, 10, 10	https://w.qualm.com/pany/jct-securitelletins/ber-20/bulleti	com /com produ ty/bu /octo	H-QUA- 031219	-
Improper	21-11-2019	10	Lack of integrity check			https:/	//ww	H-QUA-	APQ8-	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
Authenticati			allow	s MODE	I to acc	ept any	w.qual	com	031219	/1175
on			NAS n	nessages	which	can	m.com	/com		
			result	into aut	hentica	tion	pany/j	produ		
			bypas	s of NAS	in		ct-			
			_	lragon A			securit	ty/bu		
			Snapo	lragon C	ompute	,	lletins			
			_	lragon C			ber-20			
			_	lragon Ir			bulleti	n		
			^	lragon Io	•	•				
				e, Snapd	•	oice &				
				, Snapdr	•					
				ables in A	•	19,				
			_	017, AP(	•	_				
			-	096AU, A	•					
				9150, MI						
				9206, MI		•				
				9615, MI						
				9635M, I		•				
				9650, MI		•				
				8905, MS	•					
				8909W, N		•				
				3920, MS						
				8939, MS 8953, MS						
				3933, M3 3996AU,						
				ar, QCM						
				5, SC818		•				
			ĭ	45, SDM	•	•				
				50, SDM	•	•				
				36, SDM	•	•				
				10, SDM	•	•				
				10, SDM ), SDX24	•	•				
				50, SM7:	•					
			SM82		150, 5141	0130,				
				lragon_H	ligh Me	d 2016				
				.130, SX		u_2010				
				D : CVE-		289				
Integer			Buffer	overflo	w can o	ccur	https://ww			
Underflow	04 44 0040	1.0					w.qualcom		H-QUA-	APQ8-
(Wrap or	21-11-2019	4.6	while processing non- standard NAN message from					/com	031219	
Wraparound			user space. in Snapdragon					produ		-
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9207C, MDM9650, MSM8905, MSM890640, QC36174A, QC36574AU, QCA6574AU, QCA9377, QCA9377, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDA845, SDM20, SDX24, SM8150  CVE ID : CVE-2019-2297  SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Mobile, Snapdra	Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
Out-of-bounds Read  21-11-2019  Out-of-bounds Read  Out-of-Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8098, MDM9150, MDM9205, MDM9205, MDM9205, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9650, MDM9650, MDM9655,  Out-of-Snapdragon Compute, Snapdragon Huttps://www.qualcom m.com/com pany/produ ct-security/bu lletins/octo ber-2019-bulletin  Out-of-Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8098, MDM9150, MDM9205, MDM9625, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9650, MDM9655,				Electr Snapo Snapo Snapo Snapo Infras Netwo APQ8 IPQ40 MDM' MDM' MDM' MSM8 QCA6 QCA9 QCS40 SDA8 SDM8 SM81	ronics Co dragon Co dragon Indragon Wilragon Wilragon Wilragon Wilragon Wilragon Wilragon Wilragon Wilragon, Milragon, Milrago	onnective onsume adustria Mobile, Moice & Movired and APQ80 Q8053, Q8096A Q8096A Q8096A QCA617 QCA617 QCA937 N7605, SO5, SDA 636, SDI 20, SDX2	ity, r IOT, l IOT, lusic,  09,  U, Q8074, C, ), , 74A, 77, M660, M660,	securit lletins ber-20	octo 19-		
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,				com /com produ ty/bu /octo	•	•
	CV Scoring Scal	e 0-1	1-2				6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss		Description	n & CVE	Pat	ch:	NCIIP	C ID	
			MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3996AU, bar, QCM 55, SC818 45, SDM 45, SDM 710, SDM 710, SDM 710, SM7 50, SM7 150, SM7	MSM8917, SM8940, SM8976, MSM89 2150, Quantum 20, SD 429, SD 429, SD 4660, SD 46600, SD 466000, SD 466000, SD 466000, SD 466000, SD 4660000, SD 4660000, SD 4660000, SD 46600000000000000000000000000	98, CS605, A660, M439, M632, M670, M850,				
				D : CVE-						
N/A	21-11-2019	7.2	copy to the Paramare frenvire Auto, Snape Snape Snape Snape Snape Snape Snape APQ8 APQ8 APQ8 MDM MDM MSM8 MSM8	e invokin from fd of e secure la neters be om non so onment. Snapdra dragon C dragon I dragon W dragon W	or local lands ouffer, eing pope secure in Snape gon Coronsume dustria lobile, oice & Marchall (1980) (1980	ouffer ulated dragon npute, vity, r IOT, l IOT, fusic,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					ch	NCIIP	C ID
			MSM8 QCS46 SDA6 SDM6 SDM6 SDM8 SM81 Snapo	3953, MS 3996AU, 04, QCS6 60, SDA6 39, SDM 32, SDM 50, SM6 50, SM6 1ragon_F 1130, SX	MSM89 505, QM 345, SDM 1450, SD 1636, SD 1710, SD 150, SM High_Me R2130	98, 215, M429, M630, M660, M845, 7150, d_2016				
Out-of- bounds Read	21-11-2019	2.1	Trusti memo result Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 APQ8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 Snapo	ecure Kozone to ozone Maragon Adragon Maragon Wolragon Wo	do an ar which was in auto, connectionsume adustrial fobile, foice & Marian Wired and APQ80 28096, IPQ8074 SM8940, SM8940, GM8	bitrary vill vity, or IOT, l IOT, lusic, 17, 4, 4, 181, 1439, d_2016	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
msm8976			I and a second							
Loop with Unreachable Exit Condition	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop				https://w.qual m.com pany/j	com /com	H-QUA- MSM8- 031219	/1180
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ſ	Description	on & CVE	ID	Pat	ch	NCIIF	C ID
('Infinite Loop')			in Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SC818 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SDX58 SM81 Snapo	apdragor Clragon Clragon Clragon Idragon Idragon, MI 19635 M, MI 19636 M,	n Auto, ompute, onsume adustria oT, Snap dragon Vagon APQ800 DM9607 DM9607 DM9605 SM8909, MSM891 SM8953, SM895	r IOT, l IOT, dragon oice & 9, 8, 40, 7, 40, M215, A845, M450, M636, M710, X20, L50, d_2016	ct- securii lletins ber-20 bulleti	ty/bu /octo 119-		
Out-of- bounds Read	21-11-2019	10	while session messa un-int Snapo Snapo Snapo	parsing parsing on manages if netended valued tragon Caragon Caragon Caragon Caragon Iragon I	downlir gement ( etwork s ralues in uto, ompute, onsume	orta OTA ends r IOT,	https://w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	lragon Ide, Snapdor, Snapdor, Snapdor, APO 096AU, APO 09635M, Ide of Spanner, QCM, Spa	lragon V ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MSM8909, MSM8937, SM8940, SM8976, MSM8937, SM8940, SM8976, MSM8937, SM8937, SM8955 MSM8937, SM8940, SM8937, SM8940, SM8937, SM8937, SM8937, SM8940, SM8937,	7 oice & 9, 8, 5, 7, 5, 40, 5, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7,	bulleti	n		
Improper Authenticati on	21-11-2019	10	allows NAS n result bypas Snapo Snapo Snapo Snapo Snapo Mobil	of integra s MODEI nessages into aut s of NAS Iragon A Iragon C Iragon I Iragon I Iragon I ge, Snapdr	M to acc s which chentica in auto, ompute onsume ndustria oT, Snap	ept any can tion , er IOT, el IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	ables in A 017, APO 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MS 3905, MS 3905, MS 39953, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 300, SDM 45, SDM 45, SDM 45, SDM 450, SDM 710, SDM 710, SDM 710, SDM	APQ800 Q8053, APQ809 DM9607 DM9605 DM9655 MB909, MSM8916, MSM8937, GM8940, GM8976, MSM8940, GM8976, MSM89 EM8976, MSM8910, GM8976, G	9, 8, 5, 40, 5, 40, 6, 7, 68, 6805, 6860, 6832, 6832, 6850, 6850, 68150, 68150, 68150,				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM	P modulout side it received the sage. It is sage. It is sage if the sage in th	its bour res malfo in Snapo agon Cor onsume ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809	ndary ormed dragon npute, r IOT, dragon foice &	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303		
sda845					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDA8- 031219/1184

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

Weakness	Publish Date	e CVSS	1	Description	on & CVE	ID	Pat	ch:	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9650, M. 3905, M. 3905, M. 3909W, I. 3920, M. 3976, M. 3998, Nic. 2150, QC 30X, SDA 30, SDM 345, SDM 55, SM61. 50, SM8 dragon_H 1130, SX D: CVE-	5M8909, MSM8937, 5M8953, 5M8996, cobar, S605, Q 1632, SD 1632, SD 1670, SD 1850, SD 50, SM7 250, High_Me R2130	M215, A845, M450, M636, M710, X20, 150, d_2016				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	9 7.2	Out o lack of array image Snapo Snap	f bound of check of size white elf segn Adragon Adragon Offragon Maragon With the corking in 104, QCS 6, SDM 130, SM7 130, SXR D: CVE-	access definition of while reading the reading terms of the computer of the co	ue to elist ng the , , , , , , , , , , , , , , , , , , ,	https:/w.qualm.com pany/ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Time-of- check Time- of-use	21-11-2019	9 4.4	Race condition due to the lack of resource lock which will be concurrently				https:/ w.qual m.com	lcom	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pat	ch	NCIIP	CID
(TOCTOU) Race Condition			statent bound Auto, Electr Snape Snape Snape Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81	fied in the nent lead access a Snapdra conics College Iragon Irag	ds to ou in Snape igon Cor onnectiv onsume idustria oT, Snape ragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM893 Cobar, S405, Q0 60, SDA (439, SD (636, SD (636, SD	t of dragon asumer rity, er IOT, al IOT, odragon roice & 19, 18, 17, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18	pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo )19-		
Use After Free	21-11-2019	2.1	daeme static freed in Snapo Snapo Snapo Snapo Snapo Mobil Music Weara	fter free on shutd object ir from a n opdragor dragon C dragon C dragon Ir dragon Ir dragon Ic e, Snapd c, Snapdr	lown dunstance in Auto, ompute onnection on Sume on Caragon Vagon APQ800	e to getting places , vity, er IOT, al IOT, odragon oice &	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>o</sup> MDM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> SDA <sup>o</sup> SDM <sup>o</sup> SDM <sup>o</sup> SM <sup>o</sup> SM <sup>o</sup> SM <sup>o</sup> SM <sup>o</sup>	096AU, 2 9150, M 9207C, M 9650, M 8909, M 8917, M 8937, M 8996, M 8998, Ni 60, SDM 60, SDM 50, SM7 50, SXR2	DM9206 MDM960 SM8905 SM8909 SM8939, SM8953, SM8953, SM8956, SOBAT, Q B45, SDM 20, SDX 20, SDX 2130	5, 07, , , , , , , , , , , , , , , , , ,				
			varial	ole recei	ved fron	n				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	bound functi throu Auto, Snapo Snapo Snapo Snapo APQ8 APQ8 MSM8 QCA6 QCS4	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20				//ww .com ./com produ ty/bu /octo 119- n	H-QUA- 031219	
Buffer Copy without Checking	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates			w.qualcom m.com/com		H-QUA- 031219		
Size of Input			element length is greater			pany/	produ			
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
('Classic Buffer Overflow')			Snapo Snapo Snapo Snapo Snapo Snapo Snapo APQ8 MDM' MDM' MSM8 QCA6 QCA9 QCN7 SDA8 SDM8 SM81	max rate dragon A dragon C dragon C dragon In dragon I dragon V 017, APC 096AU, I 9207C, M 9650, MS 377, QCA 605, QCS 45, SDM 645, SDM 50, SMS 50, SMS	ompute onsume onnectivonsume onsume o	cr rity, er IOT, el IOT, Music in 06, 07, AU, CS605, M710, 150, R2130	ct- securii lletins ber-20 bulleti	octo )19-		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from source that the potent buffer Snape S	tmap file any un-a e, there i he bitma tially cau dragon A dragon C dragon C dragon C dragon C dragon M dragon W 016, APC 098, MD 3996AU, ar, QCS4	is a possip can use stack w. in uto, ompute onnectivonsume onsume onsume foice & March 1980 March 1	cated sibility k  k  vity, er ity, er IOT, al IOT, U,  198, 6605,	https:/ w.qual m.com pany/j ct- securif lletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDM8 SM61 SM82	45, SDM 660, SDM 45, SDM 50, SM7 50, SXR	1670, SD 1850, SD 150, SM 1130, SX	M710, X24, 8150, R2130				
Out-of- bounds Read	21-11-2019	10	Buffer while session messar un-information of Snapor Snapo	r over reparsing on manages if no tended with the decided with the decided with the decided part of the de	rad can hadownlingement of tworks walues in auto, sompute fonsume andustria of Salaragon Varagon APQ800 DM9607 DM9607 DM9605 SM8909, MSM891 SM8937, SM8940, SD808,	nappen nk OTA rends r IOT, l IOT, dragon roice & 9, 8, 6, 7, 6, 40, 6, 7, 40, 6, M439, M632, M670, M850, 6, 7,	https://w.qualm.company/jct-securitelletins/ber-20	com /com produ ty/bu /octo	H-QUA-3 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130		
			CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9625, MDM9635M, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8953, SDM630, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8- 031219/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130  CVE ID: CVE-2019-2295	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDA8- 031219/1193
			Buffer overflow can occur while processing non-	https://ww	
Integer Underflow (Wrap or Wraparound )	21-11-2019 4.6		standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDA8- 031219/1194

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			Infras Netwo APQ8 APQ8 IPQ40 MDM <sup>o</sup> MDM <sup>o</sup> MSM8 QCA6 QCA9 QCS40 SDA8	dragon Watructure orking in 017, APC 064, APC 019, IPQ8 9206, MS 9650, MS 379, QCS 379, QCS 379, QCS 379, QCS 345, SDX 50	and APQ80 AP	U, Q8074, C, , , , , , , , , , , , , , , , , ,				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear; APQ8 APQ8 MDM' MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8	P modul out side it receives sage. It sages age it sages	e may active may active smalforms mapon Corrors on Sume adustria of Snapon Corrors on Sume agon Corrors on Sume agon Corrors on Sume of Corros on Sume of Corrors on Sume of Corros on Sume of Co	ccess idary ormed dragon inpute, r IOT, dragon oice &  9,  8,  40,  7,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			QM21 SDA8- SDM6 SDM7 SDX2- SM61 SM82 Snapo	ar, QCM; 5, SC818 45, SDM 50, SDM 10, SDM 10, SDX24 50, SM7; 50, lragon_H 130, SXI D: CVE-	30X, SDA 429, SDI 630, SD 660, SD 845, SD 7, SDX55 150, SM High_Me	A660, M439, M632, M670, M850, , 8150,				
N/A	21-11-2019	7.2	copy for the Paramare from the	e invoking from fd of secure has been noned for ment. Snapdra dragon Coloragon Maragon Watructure for hing in 17, APC 1960, APC 19607, MI 19607, M	or local bouffer, eing popsecure in Snape gon Coronsume adustria lobile, oice & More and a APQ80 (8053, Q8096A) (M8909, M8909, M8940, M	ouffer oulated dragon npute, vity, r IOT, l IOT, U, 09, U, 5, 0, 98, 215, M429, M630,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-9 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE I	D	Pat	ch	NCIIP	C ID
			SDM8 SM81 Snapo , SXR1	50, SM6 50, lragon_F .130, SX	710, SDN 150, SM High_Med R2130 <b>2019-2</b> 3	7150, I_2016				
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID: CVE-2019-2329				https://w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
sdm636										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,				https://w.qualm.com/pany/jct-securityletins/ber-20	com /com produ ty/bu /octo	H-QUA- 031219	
			APQ8 APQ8 MDM9 MDM9	017, AP0 096AU, A 9150, MI 9206, MI	APQ8098 DM9205,		bulleti	n		

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9635M, I 9650, MI 8905, MS 8909W, I 8920, MS 8940, MS 8976, MS 2150, QC 80X, SDM 530, SDM 545, SDM 545, SDM 550, SM83 dragon_H	DM9655 SM8909, MSM8915 SM8937, SM8953, SM8996, Cobar, S605, Q1 660, SD 6632, SD 6670, SD 6850, SD 50, SM72 250, High_Me	AU, M215, A845, M450, M636, M710, X20,				
			Race o	<b>D : CVE-</b> condition of resour	n due to ce lock v	the				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	modification states bound Auto, Electric Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MDM MSM8 MSM8	e concur fied in the ment lead d access: Snapdra conics Co dragon I dragon	e memods to out in Snapon Coronsume on Sume on Coronsume of Coronsume	t of dragon asumer ity, r IOT, l IOT, dragon oice &	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Da	ate	cvss		Description	on & CVE	ID	Pat	:ch	NCIIP	C ID
				QM21 SDM4 SDM6 SDM7 SDX24 SM81 CVE I	D : CVE-	60, SDA 1439, SD 1636, SD 1845, SD 50, SM7: <b>2019-1</b>	845, M630, M660, X20, 150,				
Improper Validation of Array Index	21-11-20	19	4.6	occur to imparray Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 MSM8	f-bound in came proper vindex in Snapdra onics Collagon In dragon In dragon Vindex in Snapdra on Vindex in Snapdra	era drive ralidation Snapdr agon Cor onnectiv consume ndustria Mobile, Voice & M Vearable Q8017, Q8096A M9206, MDM9650 DM9650 SM8909, MSM8937, SM8937, MSM8937, MSM8937, MSM8937, MSM8937,	r due n of agon nsumer ity, r IOT, l IOT, U, 07, 07, 07, 08, 0M450, M660,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	
Out-of- bounds Read	21-11-20	19	4.6	in fast to imp while from Snapo	over-re messag proper in process firmwar dragon A	ge handlonput valing a me ing a me e in uto,	er due idation essage	https://w.qualm.com pany/jct- securitelletins	lcom l/com produ ty/bu	H-QUA- 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	:	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	1	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo APQ8 MSM8 QCN7 SDA6 SDX2	ronics Co dragon C dragon M dragon V 053, APC 3996AU, 605, QC 60, SDM 0, SDX24	onsume ndustria fobile, foice & M Q8096A MSM89 S405, Q0 636, SDI	er IOT, I IOT, Music in U, 98, CS605, M660,	ber-20 bulleti			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bi from source that to potent buffer Snape	tmap file any un-a e, there is he bitma itially care overflood dragon of dra	e is loade authentic is a possip can use stack w. in auto, ompute onnectivonsume adustria fobile, foice & MQ8096A M9205, MSM89 & 630, SD	ed cated sibility k  vity, er ity, l IOT, l IOT, Music in U, 98, 605, DA660, M636, M710, X24, 8150, KR2130	https://w.qualm.com pany/jct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while				https:/ w.qual	com	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	handl	ing WLA	4-5	5-6	m.com	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			Snape Snape Snape Snape Snape Snape APQ8 APQ8 APQ8 MDM9 MDM9 MSM8 QCA6 QCA9 SDA66 SDM6	gement for the second s	onsume onnectivonsume onsume o	er ity, er IOT, l IOT, Music in U, O7, AU, A, 7, CS605, M636, M710, 150	pany/j ct- securii lletins ber-20 bulleti	ty/bu /octo )19-		
Out-of- bounds Read	21-11-2019	10	Buffer while session messar un-interest Snaper Snaper Snaper Snaper Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM	c over reparsing on manages if netended valragon Caragon Caragon Iragon Iragon, MI 19635, MI 19635, MI 19635, MI 19650, MI 19650, MI 19650, MI 19650, MI	ad can had can	nappen nk OTA sends or IOT, l IOT, odragon oice & o o o o o o o o o o o o o o o o o o o	https:/ w.qual m.com pany/j ct- securif lletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
			MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX2 SM61 SM82 Snapo	lragon_F l 130, SX	5M8937, 5M8940, 5M8976, MSM89 2150, Q0 30X, SDA 429, SDI 6630, SD 6660, SD 845, SD 845, SD 150, SM	98, CS605, A660, M439, M632, M670, M850, ,				
Improper Authenticati on	21-11-2019	10	Lack of allow NAS result bypas Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8 MSM8	of integrals MODEN nessages into autoes of NAS dragon Adragon Coloragon Independent of the Section of the Secti	ity check M to accombined to chentical in uto, ompute onsume ot, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9625 MDM9645 SM8909, MSM891	ept any can tion  r IOT, l IOT, dragon oice &  9,  8,  7,  40,	https:/w.qualm.com pany/ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 Nicob QM21 SDA8- SDM4 SDM7 SDX20 SM61 SM82 Snapo , SXR1	lragon_H 130, SX	MSM89 2150, Qu 30X, SDA 429, SDI 630, SD 6660, SD 845, SD 2, SDX55 150, SM High_Me R2130	98, CS605, A660, M439, M632, M670, M850, 5, 8150,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape Sna	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM898, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,				//ww .com ./com produ ty/bu /octo 119- n	H-QUA-3 031219	
			Snam	lragon_F	ligh Me	d 2016				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130		
			CVE ID : CVE-2019-2295		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing non- standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM6- 031219/1207
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM6- 031219/1208
CV Scoring Scal	e 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	C ID
			APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MI 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3953, MS 3953, MS 3953, MS 36, SDM 45, SDM 45, SDM 50, SDX24 50, SM7 50, SM7	Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 GM8909, MSM8916, GM8976, MSM8976, MSM89, Q150, Q0 80X, SDA 429, SDI 8630, SDA 1660, SD 1845, SD 150, SM High_Me R2130	8, 5, 6, 40, 6, 40, 5, 7, 25, 460, M439, M632, M670, M850, 5, 8150,				
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
sdm670					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6- 031219/1210

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch:	NCIIP	C ID
			MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	3909W, 1 3920, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDM 30X, SDM 30	5M8937, 5M8953, 5M8996, cobar, 5605, Q 4660, SD 1632, SD 1670, SD 1670, SD 1850, SM7 250, High_Me R2130	AU, M215, A845, M450, M636, M710, X20, 150, d_2016				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	lack of array image Snape Snap	CVE ID: CVE-2019-2335  Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130				//ww lcom l/com produ ty/bu /octo 019- n	H-QUA- 031219	
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto,				daemon shutdown due to static object instance getting freed from a multiple places  w.qualcom m.com/com pany/produ			
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SM61 SM82	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130				ty/bu /octo )19- n		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer wlan rates elementhan rates Snapo APQ8	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,				//ww .com ./com produ ty/bu /octo 119- n	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID: CVE-2019-2251	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM6- 031219/1214
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto,	https://ww w.qualcom m.com/com pany/produ ct-	H-QUA-SDM6- 031219/1215
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			Electr Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8 QCA6 QCA9 SDA6 SDM6	dragon Conics Co	onnectivonsume ndustria Jobile, Joice & M Q8017, Q8096A M9206, MDM960 SM8996 A6174A QCA937 S405, QO	ity, or IOT, l IOT, fusic in U, O7, AU, A, 7, CS605, M636, M710,	securit lletins ber-20 bulleti	/octo )19-		
			CVE I	D : CVE-	2019-2	268				
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,				https:/ w.qual m.com pany/j ct- securing lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	į į	Descriptio	n & CVE	ID	Pat	ch	NCIIP	CID
			MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX20 SM61 SM82 Snapo	3939, MS 3953, MS 3996AU, ar, QCM 5, SC818 45, SDM 50, SDM 10, SDM 50, SM7 50, SM7 50, dragon_H	SM8976, MSM89 2150, Q0 30X, SDA 429, SDI 630, SD 660, SD 845, SD 7, SDX55 150, SM	98, CS605, A660, M439, M632, M670, M850, 5,				
Improper Authenticati on	21-11-2019	10	Lack of allows NAS in result bypas Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integrics MODEN nessages into aut is of NAS dragon A dragon C dragon Ic d	ity check M to accombined to chentical in uto, ompute onsume dustrial oT, Snap ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9645 SM8909, MSM8916, SM8940, SM8940,	k ept any can tion  r IOT, l IOT, dragon oice &  9,  8, 5, 40, 5,	https:/w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-3	
	Ì		1.101.10	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		/UI	ĺ			

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, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM898, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6- 031219/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2295		
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2303	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6- 031219/1219
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer,	https://ww w.qualcom m.com/com	H-QUA-SDM6- 031219/1220

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	ı	Description	n & CVE	ID	Pat	ch	NCIII	PC ID
			Paramare from environment of the	neters become non somment. Snapdradragon Clagon Indragon Indragon Williagon	eing pope secure in Snape gon Cor onnectivonsume ndustria lobile, oice & Maria APQ80 (28053, Q8053, Q8096A (28053, Q8064A (28053, Q8064A (28053, Q8064A (28053, Q8064A (28053, Q8064A (28053, Q8064A (28053, Q8064A (28053, Q8064A (28053, Q8064A (280	dragon npute, vity, r IOT, l I	pany/j ct- securit lletins, ber-20 bulleti	produ ty/bu /octo 119-		
Use After Free	21-11-2019	7.2	cleant missin for a f applic Comp Consu Indus	fter free up routing pointe station. in ute, Snaputrial IOT e, Snaputrial IOT	ne due to er saniti rt of a to Snapdr pdragon C, Snapdo , Snapdo	zation rusted ragon ragon ragon	https://w.qualm.com pany/j ct- securit lletins/ ber-20	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID: CVE-2019-2329	bulletin	
sdm710					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM7- 031219/1222

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130		
			CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130  CVE ID: CVE-2019-2339	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM7- 031219/1223
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM7- 031219/1224
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	ı	Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>4</sup> MSM <sup>8</sup> MSM <sup>8</sup> QCN <sup>7</sup> QM21 SDM <sup>4</sup> SDM <sup>6</sup> SDM <sup>7</sup> SDX2 <sup>4</sup> SM81	9607, MI 9650, MS 3909W, MS 3953, MS 3998, Nic 605, QCS 5, SDA6 29, SDM 32, SDM 10, SDM 4, SM615 50	5M8905 MSM8936 cobar, 5405, Q0 60, SDA 439, SD 636, SD 845, SD	, 39, AU, CS605, 845, M630, M660, X20,				
Use After Free	21-11-2019	2.1	Use and daemond static freed in Snape Snape Snape Snape Snape Snape Snape Snape Mobil Music Wears APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 SDA66 SDM6 SDM8	fter free and shutdon	issue in lown du stance gultiple in Auto, ompute, onnectivonsume industria oT, Snap ragon Vagon APQ800 Q8053, APQ809 Q805 Q805 Q805 Q805 Q805 Q805 Q805 Q805	Xtra e to getting places  vity, r IOT, l IOT, dragon oice &  9,  8,  7,  W,  AU, CS605, M450, M710, 24,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal			51.101		200,0141					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130		
1			CVE ID : CVE-2019-10490		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7- 031219/1226
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM7- 031219/1227
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch:	NCIIP	C ID
			Snapo APQ8 APQ8 MSM8 Nicob SA61! SDA8 SDM6 SDM8 SM61 SM82	50, SXR	Toice & M Q8096A M9205, MSM89 405, QCS 180X, SD 1670, SD 1670, SD 150, SM 1130, SX	U, 98, 605, DA660, M636, M710, X24, 8150,				
Out-of- bounds Read	21-11-2019	7.5	Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Out-of- bounds Read	21-11-2019	10	while sessic	r over re parsing on mana ages if ne	downlir gement (	nk OTA	https://w.qualm.com	lcom 1/com	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	I	Description	n & CVE	ID	Pat	ch	NCIII	PC ID
			un-int	ended v	alues in		ct-			
			Snapo	lragon A	uto,		securit	y/bu		
			Snapo	lragon C	ompute	,	lletins	octo/		
			•	lragon C			ber-20			
			Snapo	lragon Ir	ıdustria	l IOT,	bulleti	n		
			Snapo	lragon Io	T, Snap	dragon				
			Mobil	e, Snapd	ragon V	oice &				
				, Snapdr	_					
				ables in A	•	9,				
			_	017, APC	•					
			•	096AU, <i>I</i>	•	•				
				9150, MI						
				9206, MI						
				9615, MI		•				
				9635M, I		•				
				9650, MI		•				
				3905, MS	•					
				3909W, N		•				
				3920, MS	•					
				3939, MS	•					
				8953, MS	•					
				8996AU,						
				ar, QCM	. •	•				
			•	.5, SC818 45, SDM	•	•				
				+э, зым <sup>,</sup> 50, SDM	•	•				
				36, SDM	•	•				
				30, SDM 10, SDM	•	•				
				10, SDM ), SDX24	•	•				
				50, SM71	•	•				
			SM82		150, 5141	0130,				
				lragon_H	ligh Me	d 2016				
				.130, SXI		u_2010				
				D : CVE-		2 <b>7</b> 1				
							h++	1 /****		
				of integri	•		https:/	•		
Improper				s MODEN			w.qual			
Authenticati	21-11-2019	10		nessages into aut			m.com	-	H-QUA-	
on	21 11 2017	10				UUII	pany/p ct-	ouu ouu	031219	9/1230
<b>011</b>			bypass of NAS in Snapdragon Auto,					.,/h.,		
			_	iragon A Iragon C			securit			
CV Scoring Scale	<u> </u>				_					
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Snapo Snapo Mobil Musio Wear: APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	dragon C dragon Indragon Id dragon Id e, Snapdrables in A 017, APC 096AU, A 9150, MI 9635M, Id 9635M, Id 1395M, Id 1	onsume ndustria oT, Snap ragon Vagon APQ800 Q8053, APQ809 DM9625 DM9625 DM9655 GM8909, SM8937, SM8940, SM8976, ASM8976,	er IOT, el IOT, edragon d'oice & es	ber-20 bulleti	19-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,				https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com orodu cy/bu /octo 19-	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			Infras Netwo APQ8 MDM9 MSM8 MSM8 MSM8 QCS40 SDM4 SDM6 SDM6 SDM6 SDM8	Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID: CVE-2019-2295  SNDCP module may access array out side its boundary						
			CVE I	D : CVE-	2019-2	295				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8		its bour res malfo in Snapo agon Cor onsume ndustria oT, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9625 MDM9645 SM8909, MSM8917,	ndary ormed dragon npute, r IOT, l IOT, dragon oice & 9, 8, 5, 40, 6,	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA-3	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 Nicob QM21 SDA8- SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	3953, MS 3996AU, ar, QCM 5, SC818 45, SDM 50, SDM 10, SDM 0, SDX24 50, SM7 50, lragon_H	MSM89 2150, Q 30X, SD 429, SD 630, SD 660, SD 845, SD 50X55 150, SM	98, CS605, A660, M439, M632, M670, M850, ,				
N/A	21-11-2019	7.2	copy for the the Paramare from	invoking from fd of secure because the secure because on nones on ment. Snapdra dragon Caragon Waragon Waragon, MD 17, APC 19607, MD 19205, MD 1937, MS 1937	or local bouffer, bing pope secure in Snape on Coronsume onsume odustria dobile, oice & Maria (2006)	ouffer ulated dragon npute, vity, r IOT, I IOT, U, 09, U, 98,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-3 031219	
CV Scoring Scal					•	•	<u> </u>			ı

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDM6 SDM8 SM81 Snapo	39, SDM 32, SDM 70, SDM 50, SM6 50, dragon_H 130, SX <b>D: CVE-</b>	636, SD 710, SD 150, SM High_Med R2130	M660, M845, 7150, d_2016				
Use After Free	21-11-2019	7.2	cleand missing for a fapplic Comp Consu Indus Mobil Infras Netwo QCS40 SDM6 SDX55 SM81	ter free up routing points ailed stated ation. in ute, Snautrial IOT e, Snapd tructure orking ir 04, QCS6, SDM 5, SM615 50, SXR1 D: CVE-	ne due to er saniti ort of a tr Snapdr pdragon C, Snapdr C, Snapdr ragon W e and MDM9 605, SDA 6710, SD 50, SM72	rusted agon ragon vired 205, 845, M845, 150, R2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
qca8081										
Out-of- bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	-
			-	096AU, 1	-	ł,				

Weakness	Pul	blish Date	CVSS		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
				MSM8 MSM8 MSM8 QM21 SDM4 Snapo	3917, MS 3937, MS 3953, MS 3996AU, 55, SDM 50, SDM dragon_F	5M8940, 5M8996, QCA808 129, SDN 1632, High_Me	, 31, 4439, d_2016				
qcs404											
Use After Free	21-	11-2019	4.9	listen memo use af Snapo	equent user may repry corructer free dragon Adragon Adragon Valragon Valrag	result in uption d issue. in uto, compute connectionsume doustriate of the work of the wor	further ue to  vity, or IOT, l IOT, Music,  205, 150, R2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	lcom n/com produ ty/bu /octo	H-QUA- 031219	-
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-	11-2019	7.2	lack of array image Snapo Snap	f bound of check of size white e elf segre dragon of dra	of whilted ile reading the reading to the compute consumendustriated in MDM9	elist ng the , vity, er IOT, l IOT,	https://w.qual m.com pany/j ct- securit lletins ber-20 bulleti	lcom n/com produ ty/bu /octo	H-QUA- 031219	_
CV Scoring Scal	е	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Pu	blish Date	cvss		Description	on & CVE	ID	Pat	:ch	NCIIP	C ID
				SDM8 SM61 SXR1	570, SDM 350, SDX 50, SM7 130, SXF	24, SDX: 150, SM R2130	55, 8150,				
				CVE I	D : CVE-	2019-2	339				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-	-11-2019	2.1	to lace check buffer Snape SNAS	dragon_I	ress range the System the System to the Syst	ge sDBG , vity, or IOT, l IOT, /usic, /09, /215, /429, M630, M660, M845, d_2016	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
N/A	21-	-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon				from fd or local buffer w.qualcom m.com/com H-QUA-QCS4-om non secure ct-			•
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIF	PCID
			Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 APQ8 APQ8 MDM MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM	Snapdradragon Clagon Clagon Magon Waragon Waragon Waragon Waragon Waragon Waragon Waragon, MD 19607, MD 19	onnective on sume and ustrial flobile, foice & More of the control	vity, or IOT, l IOT, fusic,  09, U, 5, 0, 429, M429, M630, M660, M845, 7150, d_2016	lletins, ber-20 bulleti	19-		
Use After Free	21-11-2019	7.2	cleand missing for a for application Comp Consumers Indust Mobilation Infrass Netwo	fter free up routing pointed ailed station. in the trial IOT e, Snapd structure orking in 04, QCS6	ne due to er saniti art of a to Snapdr pdragon C, Snapdo Iragon V e and n MDM9	zation rusted ragon ragon ragon Vired	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE	ID	Pat	tch	NCIIP	CID
			SDM670, SDM710, SD SDX55, SM6150, SM7 SM8150, SXR1130, SX CVE ID: CVE-2019-2	150, KR2130				
sxr1130			CVE ID . CVE-2019-2	329				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Atta Reject message, Valid condition is not met resulting into an infining in Snapdragon Auto, Snapdragon Computer Snapdragon Consumers Snapdragon Industriated Snapdragon Industriated Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon Wearables in APQ800 APQ8017, APQ8053, APQ8096AU, APQ8096 MDM9150, MDM9205, MDM9206, MDM9615, MDM9607, MDM9615, MDM9635M, MDM9650, MDM9635M, MDM9650, MSM8905, MSM8909W, MSM8909W, MSM8909W, MSM8909W, MSM89137MSM8940, MSM8953MSM8976, MSM8953MSM8976, MSM8953MSM8976, MSM8996MSM8998, Nicobar, QCM2150, QCS605, QSC8180X, SDA660, SDSDM429, SDM439, SDSDM630, SDM632, SDSDM630, SDM632, SDSDM630, SDM670, SDSDM645, SDM650, SM7SM8150, SM7SM8150, SM8250, Snapdragon_High_Meg, SXR1130, SXR2130	exit ite loop  f, er IOT, el IOT, odragon oice &  99, 40, 5, 40, 5, 40, 6, 17, AU, M215, 0A845, 0M636, 0M710, 0X20, 150,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	lcom n/com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130  CVE ID: CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR1- 031219/1242
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SXR1- 031219/1243

3-4

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDM8 SM61 SM82	45, SDM 660, SDM 845, SDM 50, SM7 50, SXR2 <b>D : CVE-</b>	670, SD 850, SD 150, SM 130, SX	M710, X24, 8150, R2130				
Out-of- bounds Read	21-11-2019	10	Buffer while session messar un-information snaped Snaped Snaped Snaped Mobil Music Wear APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	r over reparsing on manages if netended with the design of	ad can hadownling gement of tworks shalues in uto, ompute onsume adustria of, Snap ragon vagon APQ800 Q8053, APQ809 DM9625 DM9625 DM9655 DM8976, SD855 DM560, SD660, SD660, SD660, SD660, SD6660, SD6660, SD6660, SD655 DM555 D	nappen nk OTA sends or IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 47, 48, 68, 68, 68, 68, 68, 68, 68, 68, 68, 6	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date CVSS Description & CVE ID		Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8937, MSM8937, MSM8937, MSM8937, MSM8937, MSM8937, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR1- 031219/1245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, SDM630, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130  CVE ID: CVE-2019-2295	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SXR1- 031219/1246
			SNDCP module may access	https://ww	
Out-of- bounds Read	21-11-2019 7.5		array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SXR1- 031219/1247

3-4

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	ables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 3905, MS 3905, MS 3	APQ800 Q8053, APQ809 DM9607 DM9605 DM9655 MB909, MSM8916, SM8937, SM8940, SM8937, SM8940, SM8937, SM8940, SM8937, SM8955 SM8956, MSM89 EMBERT SD SM8955 SM8976, MSM89 SM8955 SM8976, MSM89 SM8937, SM8	9, 8, 5, 40, 5, 40, 5, 40, 5, 98, CS605, A660, M439, M632, M670, M850, 5,				
N/A	21-11-2019	7.2	copy for the the Param are from the environment of	e invokin from fd of secure le neters be om non so onment. Snapdra dragon C dragon I dragon V dragon V dragon V structure orking in	or local bouffer, eing popsecure in Snapelogon Corsonnective onsume adustria Mobile, Voice & Movired e and	ouffer oulated dragon mpute, vity, er IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	CID
			APQ8 APQ8 MDM9 MSM8 MSM8 MSM8 MSM8 QCS49 SDM6 SDM6 SDM6 SDM8 SM81 Snapo	017, APC 096, APC 098, MD 9205, MI 9607, MI 3905, MS 3917, MS 3937, MS 3996AU, 04, QCS6 60, SDA6 39, SDM 532, SDM 570, SDM 550, SM6 1130, SXI	28096A M9150, DM9206 DM9650 M8909, M8920, M8940, M8996, MSM89 05, QM: 3450, SD 450, SD 636, SD 710, SD	5, 0, 98, 215, M429, M630, M660, M845,				
			CVE I	D : CVE-	2019-2	315				
Use After Free	21-11-2019	7.2	cleand missing for a fapplic Comp Consu Indus Mobil Infras Netwo QCS40 SDM6 SDX55 SM81	ter free to prouting points ailed station. in the station of the s	ne due to er saniti rt of a to Snapdr pdragor C, Snapdo , Snapdo ragon V e and MDM9 05, SDA 710, SD 50, SM7	zation rusted ragon ragon ragon Vired 205, 845, M845, 150, KR2130	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
sm6150										
Loop with Unreachable Exit	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met				https:/ w.qual m.com	com	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIII	PC ID
Condition			result	ing into	an infin	ite loop	pany/j	orodu		
('Infinite			in Sna	pdragor	ı Auto,		ct-			
Loop')			Snapo	lragon C	ompute	,	securit	y/bu		
			Snapo	lragon C	onsume	r IOT,	lletins	octo/		
			Snapo	lragon Ir	ndustria	l IOT,	ber-20	19-		
			Snapo	lragon Io	T, Snap	dragon	bulleti	n		
			Mobil	e, Snapd	ragon V	oice &				
			Music	, Snapdr	agon					
				ables in A	•	9,				
				017, APO	•					
			·	096AU, A	•	•				
				9150, MI						
				9206, MI						
				9615, MI		•				
				9635M, I		•				
				9650, MI		•				
				3905, MS						
				3909W, I		•				
				3920, MS	•					
				3940, MS	•					
				3976, MS		AU,				
				3998, Nic	•	W215				
			-	150, QC						
				30X, SDA						
				29, SDM						
				30, SDM	•	•				
				60, SDM 45, SDM	•	•				
				43, зрм 5, SM615	•	•				
				50, SM81	•	130,				
				lragon_H		d 2016				
				130, SX		u_2010				
			CVE I	D : CVE-	2019-2	335				
				quent us			https:/	•		
				er may r			w.qual			
				ry corru	_		m.com			<b>a.</b>
Use After	21-11-2019	4.9	use af	ter free i	issue. in		pany/j	orodu	H-QUA-	
Free			-	lragon A			ct-		031219	9/1251
				lragon C			securit			
				lragon C			lletins			
			Snapo	lragon C	onsume	r IOT,	ber-20	19-		
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)				927						

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo Infras Netwo QCS40 SM71	dragon Indragon Maragon Vertructure orking in 104, SDX 50, SM8	Mobile, Voice & M Vired e and n MDM9 55, SM61	Music, 205, 150, R2130	bulleti	n		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	CVE ID: CVE-2019-2336  Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130  CVE ID: CVE-2019-2339  Race condition due to the lack of resource lock which will be concurrently				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 <b>CVE ID : CVE-2019-2339</b> Race condition due to the lack of resource lock which				https:/ w.qual m.com pany/i ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			Wear APQ8 APQ8 MDM MDM MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7	c, Snapdr ables in A 017, APC 096AU, A 9206, MI 9607, MI 9650, MS 3909W, N 3998, Nic 605, QCS 15, SDA6 429, SDM 710, SDM 4, SM615	APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM893 SM8996, cobar, S405, Q0 60, SDA 439, SD 636, SD	8, 7C, 7C, 89, AU, CS605, 845, M630, M660, X20,				
				D : CVE-						
Use After Free	21-11-2019	2.1	daem static freed in Sna Snape Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MDM MSM8 MSM8 MSM8	fter free on shutd object in from a napdragor Caragon Caragon Indragon Indr	lown duastance grading in Auto, ompute onnectivonsume industria oT, Snap ragon Vagon APQ800 Q8053, APQ809 DM9206 GM8905 GM8905 GM8905 GM8939, GM8953, GM8952,	e to getting places  vity, r IOT, l IOT, dragon foice &  9,  8,  7,  W,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
				SDA6 SDM6 SDM8 SM61 SM82 CVE I	8998, Ni 60, SDA 60, SDM 45, SDX 50, SM7 50, SXR2 D : CVE-	345, SDM 1670, SD 20, SDX 150, SM 2130 <b>2019-1</b>	4450, M710, 24, 8150, <b>0490</b>				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11	-2019	4.6	wlan is rates element than is Snapo	•	if suppo ded rate h is grea set leng auto, compute consume onnectiv consume ndustria Mobile, Voice & N Q8053, MDM92 MDM960 SM8905 Nicobar CA6574 A9379, S405, Q0 670, SDI 20, SM6 250, SXI	rted es eter eth in r ity, r IOT, l IOT, dusic in 06, 07, , , , XS605, M710, 150, R2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11	-2019	7.2	SM8150, SM8250, SXR2130  CVE ID: CVE-2019-10566  If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute,				https://w.qualm.com pany/jct- securit lletins/ber-20	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	6-7 7-8		9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	bulletin	
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM61- 031219/1257

8-9

CV Scoring Scale

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2268		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM630, SDM630, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2271	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SM61- 031219/1258
Improper	21-11-2019	10	Lack of integrity check	https://ww	H-QUA-SM61-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
Authenticati			allow	s MODE	M to acc	ept any	w.qual	com	031219	7/1259
on			NAS n	nessages	which	can	m.com	/com		
			result	into aut	hentica	tion	pany/j	produ		
			~ ~	s of NAS			ct-			
			_	lragon A			securit			
				lragon C			lletins			
			•	lragon C		•	ber-20			
			_	lragon Ir			bulleti	n		
			^	lragon Io	•	•				
				e, Snapd	•	oice &				
				, Snapdr	•	0				
				ables in A	•	9,				
				017, AP(	•	O				
			·	096AU, <i>I</i> 9150, MI	•	•				
				9130, MI 9206, MI						
				9615, MI						
				9635M, I						
				9650, MI						
				3905, MS		•				
				3909W, I	•					
				3920, MS		•				
				3939, MS						
				3953, MS						
			MSM8	3996AU,	MSM89	98,				
			Nicob	ar, QCM	2150, Q	CS605,				
			QM21	.5, SC818	30X, SD <i>A</i>	A660,				
			SDA8	45, SDM	429, SD	M439,				
			SDM4	50, SDM	630, SD	M632,				
			SDM6	36, SDM	660, SD	M670,				
			SDM7	10, SDM	845, SD	M850,				
			SDX2	0, SDX24	, SDX55	,				
			SM61	50, SM7	150, SM	8150,				
			SM82	•						
			_	lragon_H	•	d_2016				
			, SXR1	130, SX	R2130					
			CVE I	D : CVE-	2019-2	289				
			SNDCP module may access				https:/	//ww		
Out-of-	21-11-2019	7.5	array out side its boundary				w.qual	com	H-QUA-	
bounds Read		7.10	when	it receiv	es malfo	ormed	m.com	/com	031219	9/1260
			XID m	essage.	in Snapo	dragon	pany/j	produ		
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	l	Descriptio	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	Snapdra dragon Indragon Indrag	onsume adustria of, Snap ragon Vagon APQ800 Q8053, APQ809 DM9625 MDM9655 MB9655 MB965 MB965 MB965 MB965 MB965 MB965 MB965 MB966 MSM89 MSM8	r IOT, l IOT, dragon oice & 9, 8, 40, 5, 40, 5, 40, 6, M439, M670, M632, M670, M850, ,	ct- securit lletins, ber-20 bulleti	octo 19-		
N/A	21-11-2019	7.2	copy for the to the Param are from environments Auto,	rinvokin from fd c secure l neters be om non s onment. Snapdra dragon C	or local bouffer, eing popsecure in Snapo gon Connectivon	ouffer oulated dragon npute, vity,	https://w.qual m.com pany/j ct- securit lletins/ ber-20	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315	bulletin	
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SM61- 031219/1262

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130, SXR2130		
			CVE ID : CVE-2019-2329		
sm8150					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81- 031219/1263

Weakness	Pu	blish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Use After Free	21-	-11-2019	4.9	listen memo use af Snapo	ory correcter free dragon of tructure of the off SDX5 50, SM8				//ww lcom n/com produ ty/bu /octo 019- n	H-QUA- 031219	
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-	-11-2019	7.2	CVE ID: CVE-2019-2336  Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	
Time-of- check Time- of-use (TOCTOU)	21	-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy				https:/ w.qual m.com pany/	lcom l/com	H-QUA- 031219	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	CID
Race Condition			statent bound Auto, Electr Snape Snape Snape Mobil Music Wears APQ8 APQ8 MDM' MDM' MDM' MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX24 SM81	nent lead d access Snapdra conics Co dragon Id dragon Id dragon Id e, Snapdra de, Snapdra de, Snapdra doles in 1 017, APC 096AU, 1 9206, MI 9607, MI 9650, MI 3998, Nid 605, QC 5, SDA6 29, SDM 10, SDM 10, SDM 4, SM61! 50	ds to out in Snapo agon Cor onnective consume ndustria oT, Snapo lragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM893 Cobar, S405, Q0 60, SDA 1439, SD 1636, SD 1636, SD	t of dragon sumer ity, or IOT, dragon oice & 9, 8, 7C, 9, 89, AU, CS605, 845, M630, M660, X20, 150,	ct- securit lletins, ber-20 bulleti	ty/bu /octo )19-		
Use After Free	21-11-2019	2.1	SDX24, SM6150, SM7150, SM8150  CVE ID: CVE-2019-10486  Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,				https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	096AU, 2	4-5	5-6	6-7	7-8	8-9	9-10

MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM850, SDM450, SM8250, SXR2130    CVE ID : CVE-2019-10490	Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Buffer Copy without ('Classic Buffer Overflow')  Buffer Copy without ('Classic Size of Input ('Classic Buffer Overflow')  Buffer Copy without ('Classic Size of Input ('Classic Supply Size of Input ('Classic Size of Input ('Classic Size of Input ('Classic Size of Input ('C				MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDA66 SDM6 SDM8 SM61	9207C, M 9650, MS 8909, MS 8917, MS 8937, MS 8940, MS 8996, MS 60, SDA8 60, SDA8 45, SDX	MDM960 M8905 M8909 M8939, M8953, M8953, Cobar, Q 20bar, Q 20, SDX	O7, , , , , AU, , CS605, M450, M710,				
wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8906AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130				CVE II	D : CVE-	2019-1	0490				
	without Checking Size of Input ('Classic Buffer	21-11-2019	4.6	wlan rates of eleme than me Snaped Snaped Snaped Snaped Snaped Snaped APQ80 MDM9 MSM8 QCA61 QCA70 SDA84 SDM8 SM81	module in extendant length max rate bragon A bragon Coloragon Coloragon Maragon Marago	of suppo ded rate h is great set leng uto, ompute onsume o	rted es ater gth in , er ity, er IOT, l IOT, Music in 06, 07, , 7, AU, CS605, M710, 150, R2130	w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	_	
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	CV Scoring Scal	le 0.1	1-2	7.2	2_/1	/l_5	5_6	6-7	7_0	8_0	9-10

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch	NCIIP	CID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from a source that the potent buffer Snape	tmap file any un-a e, there is he bitma tially can dragon A dragon C dragon C dragon C dragon I dragon I dragon W 016, APO 098, MD 3996AU, ar, QCS4 55P, SC8 45, SDM 60, SDM 45, SDM 50, SM7 50, SXR	uthentices a possip can use stack w. in uto, ompute onnectivonsume ondustria lobile, loice & Marco & M	cated dibility k  vity, r ity, r IOT, l IOT, l IOT, Music in U, 98, 605, DA660, M710, X24, 8150, R2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Use After Free	21-11-2019	4.6	kerne camer modu Snapo Snapo Snapo Mobil Music Weara Wired Netwo	ole doub I while has senson les power lragon A lragon I lragon I de, Snapdr ables, Sn I Infrastr orking ir 19, IPQ8	andling r and its er seque uto, onsume ndustria oT, Snap ragon agon apdrago ructure a APQ80	the sub ence in r IOT, dragon oice & on and 53,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 QCA9 SDM8 SM81	9607, MS 3909W, I 980, QCS 345, SDX 50 <b>D : CVE</b> -	Nicobar, S405, Q( 24, SM7	CS605, 150,				
Out-of- bounds Read	21-11-2019	10	while session messar un-in Snapo Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	r over reparsing on manages if netended with the design of	downlingement atwork stalues in uto, ompute onsume dustria of, Snapragon Vagon APQ800 Q8053, APQ809 QM9605	nk OTA sends or IOT, I	https:/ w.qual m.com pany/p ct- securit lletins, ber-20 bulleti	com /com orodu cy/bu /octo 19-	H-QUA-: 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, SDM850, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SM81- 031219/1272

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	Buffer overflow can occur while processing nonstandard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150  CVE ID: CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81- 031219/1273
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. 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://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SM81- 031219/1274

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch.	NCIIP	CID
			APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM7 SDX2 SM61 SM82 Snapo , SXR1	096AU, A 9150, MI 9206, MI 9615, MI 9635M, II 9650, MS 3905, MS 3905, MS 3909W, II 3920, MS 3953, MS 3953, MS 3953, MS 367, QCM 45, SC818 45, SDM 450, SDM 450, SDM 450, SDM 500, SDX24 50, SM7	APQ809 DM9205 DM9607 DM9625 MDM9655 SM8909, MSM891 SM8937, SM8940, SM8976, MSM89 2150, Q0 30X, SDA 429, SDA 5660, SD 6660, SD 6660, SD 6660, SD 6845, SD 6845, SD 6845, SD 6845, SD 6845, SD 6845, SD 6845, SD 6845, SD	8, 5, 40, 5, 40, 5, 7, 27, 28, 27, 28, 28, 38, 46, 46, 46, 46, 46, 46, 46, 46, 46, 46				
N/A	21-11-2019	7.2	copy to the Paran are from environment of Snapo	e invoking from fd of a secure be om non somment. Snapdradragon Colragon Colragon Working on Working in the corking in the cor	or local bouffer, eing popsecure in Snape onnectivonsume dustria foice & March 1980 (1980) (1	ouffer oulated dragon npute, vity, r IOT, l IOT, fusic,	https://w.qualm.com pany/jct- securitelletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Descriptio	n & CVE	ID	Pat	ch	NCIIF	CID
			MDM <sup>o</sup> MSM8 MSM8 MSM8 MSM8 QCS40 SDA60 SDM6 SDM6 SDM6 SDM8 SM81 Snapo	098, MD 9205, MI 9607, MI 8905, MS 8917, MS 8937, MS 8953, MS 8996AU, 04, QCS6 60, SDA8 39, SDM 70, SDM 70, SM6 50,	DM9206 DM9650 M8909, M8920, M8940, MSM89 05, QM2 845, SDM 450, SD 636, SD 710, SD 150, SM	98, 215, 4429, M630, M660, M845, 7150,				
			CVE I	D : CVE-	2019-2	315				
Use After Free	21-11-2019	7.2	cleand missing for a for application Compound Consumers of the Consumers o	ter free approved the province of the province	ne due to er saniti rt of a to Snapdr pdragon C, Snapdo , Snapdo ragon V and MDM9 05, SDA 710, SD 50, SM7	zation rusted ragon ragon Vired 205, 845, M845, 150,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
mdm9615										
Loop with Unreachable Exit Condition ('Infinite	21-11-2019	5	Reject condi result	process messag tion is no ing into pdragor	e, Valid ot met an infin	exit	https:/ w.qual m.com pany/j ct-	com /com	H-QUA- MDM9- 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
Loop')			Snapo Snapo Snapo Snapo Snapo Mobil Musio Wears APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SDM4 SDM6 SDM6 SDM6 SDM8 SDX58 SM81 Snapo , SXR1	dragon Colragon In dragon In dragon, In	consume ndustria oT, Snap Iragon V ragon APQ800 Q8053, APQ809 DM9607 DM9655 MB9655 MB9655, QMSM8916, SM8953, SM8956, QMSM8956, SD 1632, SD 1632, SD 1670, SD	r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 6, M215, A845, M450, M636, M710, X20, 150,	securit lletins, ber-20 bulleti	octo 19-		
Out-of- bounds Read	21-11-2019	10	while session messa un-int Snapo Snapo Snapo Snapo	parsing parsing manages if ne tended valued tragon Caragon Indragon Indrago	downlir gement ( etwork s values in tuto, compute, consume ndustria	nk OTA eends , r IOT, l IOT,	https://w.qualm.com pany/pct- securit lletins/ber-20 bulleti	com /com orodu cy/bu /octo 19-	H-QUA- MDM9- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Mobil Music Wears APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA8 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	e, Snapdr ables in A 017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 3905, MS 3905, SDM 3005, SDM 30	ragon V ragon APQ800 Q8053, APQ809 DM9607 DM9625 MDM9655 MSM8937, MSM8937, MSM8937, MSM8940, SM8940, SM8940, SM8940, SM8940, SM8955, MSM8940, SM8955, MSM8940, SM8955, MSM8940, MSM8940, MSM8955, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8955, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8940, MSM8955, MSM8940	7 oice & 7 o				
Improper Authenticati on	21-11-2019	10	allow NAS n result bypas Snapo Snapo Snapo Snapo Mobil Musio	of integra s MODEI nessages into aut ss of NAS dragon A dragon C dragon I dragon I dragon I e, Snapdr shles in A	M to acc s which chentica in uto, ompute onsume ndustria oT, Snap dragon V	ept any can tion er IOT, l IOT, odragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			APQ8 MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	lragon_F I 130, SX	APQ809 DM9205 DM9607 DM9625 MDM9655 MSM8909, MSM8916 SM8940, SM8940, SM8940, SM8940, SM8956, MSM89 2150, Qi 80X, SDA 429, SDA 429, SDA 1660, SD 1660, SD 1660, SD 1660, SD 1660, SD 1660, SD 164, SDX55 150, SM High_Me R2130	5, 7, 6, 40, 5, 40, 5, 17, 98, CS605, A660, M439, M632, M670, M850, 5,				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM	Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2289  SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Woice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,				//ww com /com produ ty/bu /octo 119- n	H-QUA- MDM9- 031219	/1280
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303		
mdm9625					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/1281

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	3905, MS 3909W, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDM 530, SDM 560, SDM 55, SM615 50, SM82 dragon_H						
Out-of- bounds Read	21-11-2019	10	Buffer while session messar un-in Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MSM8 MSM8	r over reparsing on managages if netended valragon Caragon Indragon Indrago	ad can had can	nappen nk OTA rends r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5,	https:/ w.qual m.com pany/ct- securit lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- MDM9- 031219	/1282
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	I	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 Nicob QM21 SDA8- SDM4 SDM7 SDX20 SM61 SM82 Snapo , SXR1	3953, MS 3996AU, ar, QCM; 5, SC818 45, SDM 50, SDM 10, SDM 50, SM7; 50, dragon_H 130, SX	MSM89 2150, Qu 30X, SDA 429, SDI 6630, SD 6660, SD 845, SD 150, SM High_Me R2130	98, CS605, A660, M439, M632, M670, M850, , 8150,				
Improper Authenticati on	21-11-2019	10	allowing NAS in result bypas Snapo Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integriss MODEN nessages into autors of NAS dragon A dragon College, Snapdragon In 2017, APO 096AU, A 9150, MI 9635M, I	M to accombined to accombine the computer of t	ept any can tion  r IOT, l IOT, dragon coice & 9, 8, 5, 7, 140, 15, 17, 198, 198,	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	ty/bu /octo	H-QUA- MDM9- 031219	/1283
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	5, SC81; 45, SDM 50, SDM 710, SDM 0, SDX24 50, SM7 50, dragon_H 1130, SX <b>D: CVE</b> -	429, SD 1630, SD 1660, SD 1845, SD 1, SDX55 150, SM High_Me R2130	M439, M632, M670, M850, 5, 8150, d_2016				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 MDM' MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6	P modulout side it receives age. Snapdradragon Idragon	e may a rits bound res malfolin Snapolingon Consumer and Stragon Varagon APQ800 DM9625 DM9625 DM9655	ccess ndary ormed dragon mpute, er IOT, dragon foice & e9, 8, 6, 7, 6, 17, 17, 17, 18, 17, 18, 18, 18, 18, 18, 18, 18, 18, 18, 18	https:/w.qualm.com pany/jct- securifiletins ber-20 bulleti	ty/bu /octo	H-QUA- MDM9- 031219	/1284
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303		
mdm9205					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MDM9- 031219/1285

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID: CVE-2019-2336	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/1286
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130  CVE ID: CVE-2019-2339	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/1287

Weakness	Publish Date	cvss	D	escriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	that the potential buffer of Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr APQ80 MSM89 Nicoba SA6159 SDA84 SDM66 SDM84 SM615 SM825	Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID: CVE-2019-2251				//ww com /com produ ty/bu /octo 19- n	H-QUA- MDM9- 031219	/1288
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages 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, APQ8096AU, APQ8098,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	/1289
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	lragon_F I 130, SX	DM9607 DM9625 MDM9655 SM8909, MSM891 SM8940, SM8940, SM8940, SM8940, SM8956, MSM89 2150, Qu 80X, SDA 429, SDI 1630, SD 1845, SD 150, SM High_Me R2130	7, 40, 40, 5, 7, 98, CS605, A660, M439, M632, M670, M850, ,				
Improper Authenticati on	21-11-2019	10	CVE ID: CVE-2019-2271  Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,		https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	/1290		
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130							
			CVE I	D : CVE-	2019-2	289				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8998, Nicobar, QCS404,				https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	/1291
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	05, QCS6 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM4 SDM6 SDM6 SDM8 Snapo	dragon_F	1450, SD 1636, SD 1710, SD High_Me	M630, M660, M845, d_2016				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modulout side it received ressage. Snapdra dragon Indragon Indra	its bounces malfed in Snaped agon Cordonsume industrial of The Snaped agon Waragon War	ndary ormed dragon inpute, ar IOT, I IOT, idragon foice & 9, 8, 5, 7, 6, 40, 5, 7, 6, 40, 6, 6, 4660, M439, M632, M670, M850, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	https:/w.qualm.com pany/jct-securitilletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	/1292
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch:	NCIIP	CID
			-	Snapdragon_High_Med_2016 , SXR1130, SXR2130						
			CVE I	CVE ID : CVE-2019-2303						
N/A	21-11-201	7.2	copy to the Paramare frenviro Auto, Snapo	e invoking from fd of a secure of the comment. Snapdra dragon of the comment of t	or local laborators of local laborators of secure in Snaperson Corrective on sume and striated of APQ80 (28053, 128053, 128053, 128053, 128053, 128053, 128053, 128055, 128055, 128055, 128055, 128055, 128055, 128055, 128055, 128055, 1280555, 1280555, 1280555, 1280555, 12805555, 12805555, 1	ouffer oulated dragon inpute, vity, er IOT, l IOT,	https:/w.qualm.company/jct-securitelletins/ber-20	com /com produ ty/bu /octo	H-QUA- MDM9- 031219,	/1293
Use After	21-11-2019	7.2	Use after free issue in				https:/	-	H-QUA-	
Free			cleanup routine due to				w.qual	lcom	MDM9-	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID: CVE-2019-2329	m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	031219/1294
msm8909					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MSM8- 031219/1295

4-5

6-7

7-8

8-9

9-10

5-6

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2335		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8917, MSM8939, MSM8940, MSM8933, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA645, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MSM8- 031219/1296

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM896AU, MSM8953, MSM896AU, MSM898, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20  CVE ID: CVE-2019-10503	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MSM8- 031219/1297
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MSM8- 031219/1298

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM MSM8 QCA9 SDM8 SM81	9206, M 9607, M 3909W, J 980, QC 45, SDX 50 <b>D : CVE-</b>	SM8909 Nicobar, S405, Q0 24, SM7	, CS605, 150,				
Out-of- bounds Read	21-11-2019	10	Buffer while session messar un-information snaped s	r over reparsing on manages if no detended with the design of the design	ad can hadownling gement betwork stralues in the compute consume and striation. Some and striation of the consume and striation of the consumeration of the consumerat	nappen nk OTA sends or IOT, I IOT, dragon foice & 9, 8, 5, 40, 5, 47, 48, 68, 68, 68, 68, 68, 68, 68, 68, 68, 6	https://w.qualm.com pany/jct- securing lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1299
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	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, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9640, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, SSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM630, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MSM8- 031219/1300

Weakness	Publish Date	cvss	i	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			, SXR1	130, SX	R2130					
			CVE I	D : CVE-	2019-2	289				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape SNAS	lragon_F	ress range the System the System to the Syst	ge sDBG , vity, or IOT, l IOT, dusic, 09, , CS404, 215, M429, M630, M660, M845, d_2016	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1301
			SNDCP module may access array out side its boundary				https:/ w.qual	com		
Out-of- bounds Read	21-11-2019	7.5	when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &				m.com pany/p ct- securit lletins, ber-20 bulleti	cy/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	c, Snapdr ables in A 017, APC 096AU, A 9150, MI 9206, MI 9635M, I 9635M, I 39650, MS 3909W, I 3920, MS 3939, MS 3939, MS 3953, MS	APQ800 Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 GM8909, MSM8937, GM8976, MSM8976, MSM89, Q150, Q0 80X, SDA 429, SDI 1630, SD 1845, SD 150, SM High_Me R2130	8, 5, 40, 6, 40, 7, 27, 27, 4660, M439, M632, M670, M850, ,				
N/A	21-11-2019	7.2	copy for the the Paramare from the environment of t	e invoking from fd of secure le neters be om non so onment. Snapdra dragon C dragon Indragon V dragon V dragon V	or local bouffer, eing popsecure in Snape connectionsume dustria dobile, foice & M	ouffer oulated dragon npute, vity, r IOT, l IOT,	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2315		
mdm9655					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MDM9- 031219/1304

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9650, MI 3905, MS 3909W, NS 3920, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDM 30X, SDM 360, SDM 345, SDM 345, SDM 345, SM615 1130, SX	5M8909, MSM8915, SM8953, SM8996, cobar, S605, Q 439, SD 6632, SD 6632, SD 6670, SD 50, SM7 250,	AU, M215, A845, M450, M636, M710, X20,				
			CVE I	D : CVE-	2019-2	335				
Out-of- bounds Read	21-11-2019	10	while session messar un-introduced Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MDM MDM MDM MDM MSM8 MSM8	r over reparsing manages if netended valuagen Caragon Caragon Internation Inte	downlingement of the twork status in the two computes on sume adustria of the two consumeragon Wagon APQ800 Q8053, APQ809 DM9605 DM9600	nk OTA Sends  r IOT, I IOT, dragon Soice &  9,  8, 5, 7, 40, 6,	https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- MDM9- 031219	/1305
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	į į	Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX20 SM61 SM82 Snapo	3939, MS 3953, MS 3996AU, ar, QCM 5, SC818 45, SDM 50, SDM 710, SDM 710, SDM 50, SM7 50, dragon_H 1130, SXI	SM8976, MSM89 2150, Q0 30X, SDA 429, SDI 630, SD 660, SD 845, SD 7, SDX55 150, SM	98, CS605, A660, M439, M632, M670, M850, 5,				
Improper Authenticati on	21-11-2019	10	Lack of allows NAS in result bypas Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	of integrics MODEN nessages into aut is of NAS dragon A dragon C dragon Ic dragon Ic dragon Ic dragon Ic e, Snapdr ables in A 9150, MI 9206, MI 9635M, I 9635M, I 9635M, I 89650, MI 8905, MS 8909W, N 8920, MS 8939, MS	ity check M to accombined to chentical in uto, ompute, onsume adustria oT, Snap ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MDM9625 MDM9625 MDM9625 MB909, MSM8916, SM8940, SM8940,	keept any can tion  Triot, lot, lote & ept any can tion  Soice & ept any can tion  8, control of the control of	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219,	/1306
	e 0.4		MSMg	JJJOAU,	MOMBA	70,				

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			QM21 SDA8 SDM4 SDM7 SDX2 SM61 SM82 Snapo	ar, QCM 15, SC81; 45, SDM 150, SDM 10, SDM 10, SDX24 50, SM7 50, dragon_H 1130, SX <b>D: CVE-</b>	80X, SDA 429, SDA 1630, SDA 1660, SDA 1845, SDA 150, SMA High_Me R2130	A660, M439, M632, M670, M850, , 8150,				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modulout side it receive essage. Snapdradragon Idragon Idrag	e may a its bounters malfolia Snapolia	ccess ndary ormed dragon npute, r IOT, dragon oice &  9,  8,  7,  40,  6,  47,  48,  CS605, A660, M439, M632,	https:/w.qualm.company/jct-securitelinsber-20bulleti	ty/bu /octo	H-QUA- MDM9- 031219	/1307
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	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, SM8250, Snapdragon_High_Med_2016, , SXR1130, SXR2130 CVE ID: CVE-2019-2303		
mdm9635m					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MDM9- 031219/1308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9640, MDM9635M, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8953, SDM450, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM645, SDM650, SDM710, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MDM9- 031219/1309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130		
			CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM630, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MDM9- 031219/1310

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Out-of- bounds Read	21-11-2019	7.5	array when XID n Auto, Snape Snape Snape Mobil Music Wear APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	P modulout side it receive nessage. Snapdradragon Idragon Idragon, Martin School, Martin School, Martin School, Martin School,	e its bount res malforin Snapon Corromsume industria oT, Snapol ragon Vagon APQ800 DM9605 DM9605 DM9605 DM9655 SM8909, MSM8937, SM8940, SM8976, MSM8976, MSM	ndary ormed dragon inpute, er IOT, el	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com orodu cy/bu /octo 19-	H-QUA- MDM9- 031219	/1311
qca9980	,									
Use After Free	21-11-2019	4.6	kerne	ble doub el while h ra senso	nandling	the	https:/ w.qual m.com	com	H-QUA-QCA9- 031219/1312	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150  CVE ID: CVE-2019-2266	pany/produ ct- security/bu lletins/octo ber-2019- bulletin	
qm215					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QM21- 031219/1313

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	ı	Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			MSM8 MSM8 QCM2 SC818 SDM4 SDM6 SDM6 SDM8 SDX5! SM81 Snapo	3920, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDA 30, SDM 30, SDM 45, SDM 5, SM615 50, SM82 dragon_H	5M8953, 5M8996, cobar, S605, Ql 660, SD 6439, SD 6670, SD 6850, SD 50, SM72 250, High_Me R2130	M215, M215, A845, M450, M636, M710, X20, 150,				
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race of lack of will be modificated bound Auto, Electry Snaper Sn	condition of resource e concur fied in the ment lead d access in Snapdra conics Co dragon In dragon In dra	n due to ce lock verently e memo ds to out in Snapo gon Cor onnective onsume dustria oT, Snap ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM893 cobar, S405, Q0	the which apy tof dragon asumer ity, at IOT, adragon oice & 19, 100, 100, 100, 100, 100, 100, 100,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-031219	•
			סואועט	32, SDM	636, SD	M660,		l		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM63	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-QM21- 031219/1315

Weakness	Publish Date CVSS Description & CVE ID		Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130		
			CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QM21- 031219/1316

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch:	NCIIF	PC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape SDM6 SDM6 SDM6 SDM6 SDM8 Snape , SXR2	lragon_H	ress range the System to, code. in uto, ompute onnectivonsume industrial lobile, coice & March 1980, SM8905, SM8905, SM8937, SM8937, SM8953, S	ge sDBG , vity, er IOT, l IOT, Music, 09, , , , , , , , , , , , , , , , , ,	https:/w.qualm.com/pany/ct-securilletinsber-20	com /com produ ty/bu /octo	H-QUA- 031219	=
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Mobil Music Wear	P modulout side it receives sage. It sagon Caragon Ir dragon Ir dragon Ir dragon Ir sagon Ir	its bounges malfolin Snapon Coronsume adustria oT, Snapon Vagon APQ800	ndary ormed dragon npute, er IOT, d IOT, odragon oice &	https:/ w.qual m.com pany/ct- securi lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch.	NCIIP	CID
			MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM7 SDX2 SM61 SM82 Snapo , SXR1	096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MI 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 3053, MS 305	DM9205 DM9607 DM9625 MDM964 DM9655 GM8909, MSM891 GM8976, GM89	5, 7, 6, 40, 5, 17, 98, CS605, A660, M439, M632, M670, M850, 5,				
N/A	21-11-2019	7.2	copy to the Paran are from environment of Snapo	e invoking from fd of secure lands on non soment. Snapdradragon Colragon Maragon Working on Working in 17, APO 1996,	or local bouffer, eing popsecure in Snape onnectivonsume dustria foice & March 1980 (1980) (1	ouffer oulated dragon mpute, vity, er IOT, l IOT, fusic,	https://w.qualm.com pany/jct- securite lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130		
Out-of- bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QM21- 031219/1320

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIP	CID
			CVE I	D : CVE-	2019-2	318				
sm7150										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi- result in Sna Snapo Snapo Snapo Snapo Snapo Mobil Music Weara APQ8 APQ8 MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SDM6 SDM6 SDM6 SDM6 SDM8 SDX58 SNapo SNapo SNapo SNapo MSM8 SDM6 SDM6 SDM8 SDX58 SNapo SNapo SNapo SNapo SNapo SNapo SNapo MSM8 MSM8 SNapo S	e process t messag tion is n cing into apdragon of dragon of solution dragon of dragon of solution dragon dragon of solution dragon drago	ge, Valid ot met an infin n Auto, compute consume ndustria oT, Snap dragon APQ800 Q8053, APQ809 DM9607 DM9607 DM9655 SM8909, MSM891 SM8953, SM	exit ite loop , er IOT, l IOT, dragon oice & e9, 8, 5, 7, 5, 40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150, d_2016	https://w.qualm.com/pany/jct-securit/lletins/ber-20	com /com produ ty/bu /octo	H-QUA- 031219	/1321
Use After Free	21-11-2019	4.9		quent u			https:/	•	H-QUA- 031219	
			nsten	er may r	esuit in	iurtner	w.qual	com	031219	11044
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			use af Snapo Snapo Snapo Snapo Snapo Snapo Infras Netwo QCS40 SM71	ory corructer free in the fragon Coloragon Coloragon Magon Working in the fragon Working in the forking in the	issue. in uto, ompute onnectiv onsume ndustria fobile, oice & N Vired and MDM9 55, SM61	, vity, er IOT, d IOT, Music, 205, 150, R2130	m.com pany/j ct- securit lletins ber-20 bulleti	produ ty/bu /octo 119-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	lack of array image Snape Snap	f bound a f check of size white e elf segn dragon C dragon C dragon In dragon In dragon W dragon W dragon W dragon W dragon SDM 504, QCS6 50, SDM 50, SDM	of whilted le readinents. in uto, omputed onsumed industrial lobile, Vired and in MDM9 in MDM9	elist ng the  , vity, er IOT, al IOT, M845, M845, 55, 8150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Time-of- check Time- of-use (TOCTOU) Race Condition	21-11-2019	4.4	lack o will be modif staten	condition f resource e concur fied in the nent lead	ce lock v rently e memo ds to ou	which py t of	https://w.qual m.com pany/j ct- securit	com /com produ	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[	Description	on & CVE	ID	Pat	ch	NCIIP	CID
			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, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150  CVE ID: CVE-2019-10486  Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Hong Snapdragon Consumer IOT, Snapdragon Industrial IOT, Sulletin  bulletin  bulletin  bulletin  bulletin  bulletin  bulletin  bulletin							
Use After Free	21-11-2019	2.1	daemo static freed in Sna Snapo Snapo Snapo Snapo Snapo Mobil Music Weara APQ8 APQ8 MDM9	on shutd object ir from a n ipdragor Iragon C Iragon C	lown dunstance grant properties on sume andustria properties on Vagon APQ800 Q8053, APQ809 DM9206	e to getting places vity, r IOT, l IOT, dragon oice &	w.qual m.com	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM8 SM61 SM82	9650, M3 8909, MS 8917, MS 8937, MS 8940, MS 8998, Ni 660, SDA 660, SDA 645, SDX 50, SM7 50, SXR2	5M8909 5M8920, 5M8939, 5M8953, 5M8996, cobar, Q 345, SDN 1670, SD 20, SDX 150, SM	W, , , AU, CS605, M450, M710, 24, 8150,				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bi from a source that the potent buffer Snape Sna	tmap file any un-a e, there he bitma tially car coverflo dragon C dragon C dragon C dragon I dragon I dragon W 016, APC 098, MD 3996AU, ar, QCS4 55P, SC8 45, SDM 660, SDM 50, SM7 50, SXR2 D: CVE-	e is load authenticis a possip can use stactive. In auto, ompute onnective onsume adustria fobile, foice & MQ8096A M9205, MSM89 & MSM8	ed cated sibility k  vity, er city, l IOT, l IOT, Music in U, 98, 6605, DA660, M636, M710, X24, 8150, X2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Use After	21-11-2019	4.6	Possible double free issue in				https:/	//ww	H-QUA-	SM71-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
Free			camer modu Snapo Snapo Snapo Mobil Music Weara Wired Netwo IPQ40 MDM0 MDM0 MSM8 QCA9	l while he a sensor les power lagon Chagon Ideagon Ide	r and its er seque uto, onsume dustria oT, Snap ragon apdrago apdrago APQ80 3064, DM9207 SM8909 Vicobar, S405, Q0	ence in or IOT, of IOT, of agon of oice & on and 53, of, ccs605,	w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	031219	/1327
			CVE I	D : CVE-	2019-2	266				
Out-of- bounds Read	21-11-2019	10	while session messar un-interest Snape Snape Snape Snape Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM	over reparsing manages if netended valuaging Caragon Caragon In the Caragon In th	downlingement of tworks alues in uto, ompute onsume ndustria oT, Snapragon Vagon APQ800 Q8053, APQ809 DM9605 DM9625 DM9655 DM9655 DM9655	nk OTA Sends  or IOT, I IOT, I IOT, or oice &  9, 8, 6, 7, 6, 40, 6,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch.	NCIIP	C ID
			MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX2 SM61 SM82 Snapo	3909W, N 3920, MS 3939, MS 3953, MS 3996AU, ar, QCM 55, SC818 45, SDM 50, SDM 710, SDM 710, SDM 750, SM7 50, dragon_H 1130, SXI	5M8937, 5M8940, 5M8976, MSM89 2150, Q0 30X, SDA 429, SDI 6630, SD 6660, SD 845, SD 845, SD 150, SM	98, CS605, A660, M439, M632, M670, M850, ,,				
Improper Authenticati on	21-11-2019	10	Lack of allow NAS result bypas Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MSM8 MSM8	of integris MODEN nessages into aut is of NAS dragon A dragon C dragon Ir dr	ity check M to accombined to chentical in uto, ompute onsume ot, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9625 MDM9645 SM8909, MSM891	ept any can tion  r IOT, l IOT, dragon oice &  9,  8,  7,  40,  6,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	n & CVE	ID	Pat	ch	NCIIP	CID
			MSM8 Nicob QM21 SDA8- SDM4 SDM7 SDX20 SM61 SM82 Snapo , SXR1	3953, MS 3996AU, ar, QCM 5, SC818 45, SDM 50, SDM 10, SDM 50, SM7 50, SM7 1ragon_H 130, SX	MSM89 2150, Q 30X, SDA 429, SDA 630, SD 660, SD 845, SD 5, SDX55 150, SM ligh_Me R2130	98, CS605, A660, M439, M632, M670, M850, ,				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modulout side it receives age. It sages age. It sages age and age	its bounders malfoling Snapoling Corsume and ustria port, Snapoling Snapolin	ndary ormed dragon npute, r IOT, d IOT, dragon oice & 9, 8, 6, 7, 7, 7, 98, CS605, A660,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-3 031219	
CV Scoring Scale	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR2	lragon_H 1130, SX <b>D : CVE-</b>	660, SD 845, SD 5, SDX55 150, SM High_Me R2130 <b>2019-2</b>	M670, M850, 8150, d_2016				
N/A	21-11-2019	7.2	copy to the Paramare frenvire Auto, Snape	e invoking from fd of secure lands and secure lands on ment. Snapdradragon Caragon Indragon Varagon Varagon, APO 19205, MS 1937, MS 193	or local louffer, eing popsecure in Snapgon Coronsume industria lobile, loice & Marie and loice &	ouffer oulated dragon mpute, vity, or IOT, l IOT, U, o, o, o, o, o, means Mass, Mass, Mass, Mass, Mass, Mass, Mass, Mass, Mass,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-3 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ı	Description	n & CVE	ID	Pat	ch	NCIIP	CID
			-	lragon_F I 130, SX	_	d_2016				
			CVE I	D : CVE-	2019-2	315				
Use After Free	21-11-2019	7.2	cleand missing for a fapplic Comp Consu Indus Mobil Infras Netwo QCS40 SDM6 SDX55 SM81	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID: CVE-2019-2329			https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	ty/bu /octo	H-QUA-3	
sdm429										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi- result in Sna Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9	Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Waarablas in APOS000			https:/ w.qual m.com pany/ ct- securi lletins ber-20 bulleti	ty/bu /octo	H-QUA-3	
CV Scoring Scal (CVSS)	e 0-1	1-2	MSM8905, MSM8909, 2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Dat	te CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	3909W, 1 3920, MS 3940, MS 3976, MS 3998, Nic 2150, QC 30X, SDM 229, SDM 30, SDM 345, SDM 55, SM61: 50, SM8 dragon_H	5M8937, 5M8953, 5M8996, cobar, S605, Q 1632, SD 1632, SD 1670, SD 1850, SM7 250, High_Me	M215, A845, M450, M636, M710, X20,				
				D : CVE-						
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-201	9 4.4	lack of will be modificated and will be modificated an	condition of resour econcur fied in the ment lead access Snapdra conics College, Snapdra dragon Idragon Idrago	ce lock werently the memory ds to out in Snapel agon Connective onsume adustria oT, Snapel agon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM893 cobar, S405, Q0 60, SDA	which  py t of dragon nsumer ity, or IOT, l IOT, dragon foice &  9,  8, 7C, 0, , 39, AU, CS605, 845,	https:/ w.qual m.com pany/i ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

			SDM7	32, SDM 10, SDM 4, SM61! 50	1845, SD	X20,				
			CVE I	D : CVE-	2019-1	0486				
Out-of- bounds Read	21-11-2019	10	while session messar un-introduced snaped sn	r over reparsing on manages if netended with the sended with the sended with the sended reparsion of t	downling gement of the etwork strainers in auto, compute of the etwork straine	nk OTA sends  ir IOT, I IOT, I IOT, dragon oice &  9,  8,  7,  40,  5,  40,  6,  M439, M632, M670, M850,  8150,	https:/w.qualm.company/jct-securitilletins/ber-20bulleti	com /com produ ty/bu /octo	H-QUA-3 031219	
CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909W, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4- 031219/1336
CV Scoring Scal	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

(CVSS)

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch:	NCIIF	PC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape SDM6 SDM6 SDM6 SDM6 SDM8 Snape , SXR2	lragon_H	ress range the Systode. in uto, ompute onnectivonsume dustria lobile, oice & Marcolon (2005), SM8905, SM8905, SM8937, SM8953,	ge DBG  vity, r IOT, l IOT, 4usic, 09, , CS404, 215, M429, M630, M660, M845, d_2016	https:/ w.qual m.com pany/s ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Mobil Music Wear	P modul out side it receiv lessage. i Snapdra dragon C dragon Ic dragon Ic e, Snapd c, Snapdra	its bour res malfo gon Cor onsume ndustria oT, Snap ragon V ragon	ndary ormed dragon npute, r IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch.	NCIIP	CID
			MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MI 8905, MS 8905, MS 8920, MS 8939, MS 8953, MS 8953, MS 8953, MS 636, SDM 636	DM9205 DM9607 DM9625 MDM964 DM9655 GM8909, MSM891 GM8976, GM89	5, 7, 6, 40, 6, 40, 7, 7, 27, 28, 28, 28, 38, 46, 46, 46, 46, 46, 46, 46, 46, 46, 46				
N/A	21-11-2019	7.2	copy to the Param are from environment of Snapo	e invoking from fd of a secure be om non somment. Snapdradragon Colragon Colragon Working on Working in the corking in the cor	or local bouffer, eing popsecure in Snape onnectionsume adustria foice & March 1980 (1980) (1	ouffer oulated dragon npute, vity, r IOT, l IOT, fusic,	https://w.qualm.com pany/jct- securite lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130		
Out-of- bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4- 031219/1340

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	CID
			CVE I	D : CVE-	2019-2	318				
sdm632	L									
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi- result in Sna Snapo Snapo Snapo Snapo Snapo Mobil Musio Weara APQ8 APQ8 MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SDM6 SDM6 SDM6 SDM6 SDM8 SDX58 SNapo SNapo SNapo SC818 SDM6 SDM6 SDM8 SDX58 SNapo SNapo SNapo SNapo SNapo SNapo SNapo MSM8 SNapo	process t messag tion is no ing into apdragon C dragon In dragon, MI dragon, MI dragon, MI dragon, SD dragon, SD dragon, In dragon, SD d	re, Valid of met an infin in Auto, ompute onsume industria oT, Snap ragon Vagon APQ809 DM9607 DM9607 DM9605 SM8909, MSM8913, SM8953, S	exit ite loop , er IOT, l IOT, dragon oice & e9, 8, 5, 7, 5, 40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150, d_2016	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Time-of-	21-11-2019	4.4	Race condition due to the			https:/	•	H-QUA- 031219		
check Time-	e		lack of resource lock which			w.qual				
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
of-use (TOCTOU) Race Condition			modification states bound Auto, Electric Snape Snape Snape Mobil Music Wears APQ8 MDM MDM MDM MSM8 MSM8 MSM8 QCN7 QM21 SDM4 SDM6 SDM7 SDX2 SM81	e concur fied in the ment lead d access Snapdra fonics Con dragon In dragon In dragon In dragon In dragon In dragon In e, Snapdra bles in In 017, APO 096AU, In 9206, Min 9607, Min 9650,	te memo ds to out in Snapo agon Cor onnectiv consume ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9207 DM9640 SM8905 MSM890 MSM80 MSM80	t of dragon asumer ity, r IOT, IOT, dragon foice & 9, 8, 7C, 9, 845, M630, M660, X20, 150,	m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo		
Out-of- bounds Read	21-11-2019	10	while session messa un-inte Snapo Snapo Snapo Snapo Snapo Mobil Musio	r over re parsing on manag ages if ne tended v dragon C dragon C dragon I dragon I c, Snapdr ables in J	downlingement (setwork stralues in total), compute, consumerate of T, Snap dragon V	nk OTA eends  r IOT, I IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ſ	Description	on & CVE	ID	Pat	ch	NCIIP	CID
			APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	017, APC 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9650, MS 8905, MS 8920, MS 8939, MS 8953, MS 895	APQ809 DM9205 DM9607 DM9625 MDM9655 MSM8909, MSM8916 SM8940, SM8940, SM8940, SM8940, SM8956, MSM89 2150, Qi 80X, SDA 429, SDA 429, SDA 1660, SD 1660, SD 1660, SD 1660, SD 1660, SD 1660, SD 164, SDX55 150, SM High_Me R2130	5, 7, 5, 40, 5, 17, 98, CS605, A660, M439, M632, M670, M850, 5,				
Improper Authenticati on	21-11-2019	10	allows NAS n result bypas Snape Snape Snape Snape Snape Mobil Music Wears APQ8 APQ8	of integrals MODEI nessages into aut s of NAS lragon A lragon C lragon I lragon I g, Snapdr ables in A 017, APO 096AU, A	M to acc s which chentica in outo, ompute onsume ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809	ept any can tion  To IOT, dragon oice & 9,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch.	NCIIP	CID
			MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR2	9206, MI 9615, MI 9635M, I 9650, MS 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3996AU, bar, QCM 55, SC818 45, SDM 45, SDM 45, SDM 710, SDM 710, SDM 710, SDM 710, SM7 50, SM7 50, SM7 130, SX	DM9625 MDM9655 MB909, MSM8915 SM8937, SM8976, MSM89 2150, Q0 80X, SDA 429, SDA 6630, SD 6660, SD 6845, SD 6845, SD High_Me R2130	5, 40, 5, 17, 98, CS605, A660, M439, M632, M670, M850, 5,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape Snape Snape Snape Snape Snape Snape Snape Snape Model MSM8 MSM8	mation d k of addr done or rs in SDI dragon C dragon C dragon Ir dragon V dragon V dragon V structure orking ir 017, APO 9205, MS 3909, MS	ress range the System the System to the Syst	ge sDBG  vity, or IOT, l IOT, fusic,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			QCS4 SDA6 SDM6 SDM6 SDM6 SDM8 Snapo	dragon_F	505, QM: 345, SDN 1450, SD 1636, SD 1710, SD High_Me	215, M429, M630, M660, M845, d_2016				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	P modulout side it received ressage. Snapdra dragon Idragon Id	its bounders malfolin Snapolingon Consumer industria oT, Snapolingon Veragon Veragon Veragon Veragon Veragon Veragon Veragon MP 9605 M	ndary ormed dragon mpute, er IOT, dragon foice & 9, 8, 5, 40, 5, 40, 5, 4660, M439, M632, M670, M850, M850,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-3	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness N/A	21-11-2019	7.2	SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2303  While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo	H-QUA-SDM6- 031219/1347
N/A	21-11-2019	7.2	APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650,	ct- security/bu	_

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6- 031219/1348
11151110917	T				
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MSM8- 031219/1349

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>o</sup> MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9615, MI 9635M, I 9635M, I 9650, MS 3905, MS 3909W, I 3976, MS 3976, MS 3976, MS 3998, Nic 2150, QC 30X, SDM 530, SDM 545, SDM 545, SDM 545, SDM 545, SM615 1130, SXI	MDM9655 M8909, MSM8915 M8953, M8953, M8966 Cobar, S605, Q 6632, SD 6632, SD 6670, SD 6630, SM7 250, High_Me R2130	40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150,				
Use After Free	21-11-2019	2.1	Use and daem static freed in Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MSM8 MSM8	D: CVE- fter free on shutd object ir from a n apdragon C dragon C dragon Ic dragon Ic dragon Ic e, Snapdr ables in A 017, APC 096AU, A 9150, MI 9207C, M 9650, MS 3909, MS	issue in lown du stance in Auto, ompute onnectionsume on Vagon APQ800 Q8053, APQ809 DM9206 SM8905 SM8905 SM8905 SM8905 SM8905 SM8920,	Xtra e to getting places  vity, er IOT, el IOT, edragon oice & e9, 8, 6, 7, , W,	https:/w.qualm.com pany/ct- securi lletins ber-20 bulleti	ty/bu /octo	H-QUA- MSM8- 031219	/1350
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 SDA6 SDM6 SDM8 SM61 SM82	3940, MS 3996, MS 3998, Nic 60, SDA 660, SDM 345, SDX 50, SM7 50, SXR2	5M89962 cobar, Q 345, SDN 1670, SD 20, SDX 150, SM	AU, CS605, 1450, M710, 24, 8150,				
Improper Validation of Array Index	21-11-2019	4.6	Out-o occur to imparray Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 SDX2	f-bounds in came proper verindex in Snapdra conics Codragon In dragon In dragon W 009, APO 053, APO 098, MD 9207C, M 9640, MI 3905, MS 3909W, M 3920, MS 3940, MS 3940, MS	s access ra drive alidation Snapdragon Coronsume ndustria Mobile, Toice & Moserable Q8017, Q8096Al M9206, MDM9650 DM9650 DM9650 DM9650, MSM891, SM8937, SM8933, MSM894660, SE	can r due n of agon sumer ity, r IOT, I IOT, fusic, s in J, 7, 7, 7, 98, 0M450, M660,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1351
Out-of- bounds Read	21-11-2019	10	while sessic messa un-in	r over re parsing on manag ages if ne tended v dragon A	downlir gement ( etwork s values in	ık OTA	https://w.qualm.company/j	com /com produ	H-QUA- MSM8- 031219	/1352
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musio Wears APQ8 MDMS MDMS MDMS MSM8 MSM8 MSM8 MSM8 MSM	dragon C dragon In dragon In dragon In dragon Io e, Snapdr ables in Io 017, APO 096AU, Io 9615, MI 9615, MI 9635M, Io 9650, MI 3905, MS 3905, SDM 450, SDM	ompute, onsume industria oT, Snap dragon Vagon APQ800 Q8053, APQ809 DM9605 DM8906 DM9605 DM9606 DM96	r IOT, l IOT, dragon oice & 9, 8, 40, 40, 7, 40, M439, M632, M670, M850, , 8150,	lletins, ber-20 bulleti	19-		
Improper Authenticati on	21-11-2019	10	allow NAS result bypas Snapo Snapo Snapo	of integras MODEI nessages a into aut as of NAS dragon A dragon C dragon C	M to accommodate which of the conticate of the conticate of the continuation of the co	ept any can cion r IOT,	https://w.qual m.com pany/j ct- securit lletins/ ber-20	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ſ	Description	on & CVE	ID	Pat	ch	NCIII	PC ID
			Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	dragon Ide, Snapda, Snapda, Snapda, Description of the street of the str	lragon V ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MSM8909, MSM8937, SM8940, SM8976, MSM8937, SM8940, SM8976, MSM8937, SM8937, SM8955 MSM8937, SM8937,	7 oice & 9, 8, 5, 7, 5, 40, 5, 7, 6, 7, 6, 7, 6, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7,	bulleti	n		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape Snape Snape Snape Snape Snape Snape Snape Snape	mation d k of addr done or rs in SDI dragon C dragon C dragon I dragon W dragon W	ress range the System code. in uto, ompute onnection onsume adustria fobile, foice & M	ge sDBG , , vity, er IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	I	Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			Netwo APQ8 MDM <sup>0</sup> MSM8 MSM8 MSM8 QCS40 SDA6 SDM6 SDM6 SDM6 SDM8 Snapo	lragon_H	APQ80 Q8053, SM8905 M8917, SM8937, SM8953, cobar, Q 05, QM2 845, SDM 450, SD 710, SD	CS404, 215, 4429, M630, M660, M845,				
Out-of- bounds Read	21-11-2019	7.5	SNDC array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear; APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8 MSM8	P modul out side it receiv essage. is Snapdra dragon Ir	e may active may active smalforms mapped on consume adustria of the consume of th	ccess idary ormed dragon inpute, r IOT, dragon oice &  9,  8,  40,  7,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1355
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	CID
			QM21 SDA8 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	lragon_H 130, SXI <b>D : CVE</b> -	30X, SDA 429, SDI 630, SD 660, SD 845, SD 7, SDX55 150, SM High_Me R2130	A660, M439, M632, M670, M850, , 8150, d_2016				
N/A	21-11-2019	7.2	copy for the Paramare from the	e invoking from fd of secure has been noned for ment. Snapdra dragon Coloragon Maragon Watructure for hing in 17, APC 1960, APC 19607, MI 19607, M	or local bouffer, eing popsecure in Snape gon Coronsume adustria lobile, oice & Maried and a APQ80 (28053, 28096A) (28096A) (2809	ouffer oulated dragon npute, vity, r IOT, l IOT, U, 09, U, 0, 04, 05, 04, 08, 09, 09, 09, 09, 09, 09, 09, 09, 09, 09	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219,	/1356
CV Scoring Scale	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	l	Description	on & CVE	ID	Pat	ch.	NCIIP	C ID
			SDM8 SM81 Snapo , SXR1	70, SDM 50, SM6 50, dragon_F 130, SX <b>D : CVE-</b>	150, SM High_Me R2130	7150, d_2016				
Out-of- bounds Read	21-11-2019	2.1	Non S Trust memo result Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo Metwo APQ8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MS	ecure Kozone to ozy read into DO dragon Adragon Chagon Indragon Witragon Witructure O53, APO 096AU, MS 3937, MS 3996AU, S, SDM 4-50, SDM dragon_F	ernel can do an ar which v S in auto, connecti- consume ndustria Mobile, Yoice & M Vired and APQ80 Q8096, IPQ8074 SM8940, SM8940, QCA808 QCA808 429, SDM	n cause bitrary vill vity, er IOT, l	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- MSM8- 031219	/1357
msm8920			1							
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &				message, Valid exit tion is not met ing into an infinite loop pdragon Auto, lragon Compute, lragon Industrial IOT, lragon IoT, Snapdragon intups://w w.qualcon m.com/cc pany/pro ct- security/l lletins/oc ber-2019 bulletin			/1358
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Music Wear APQ8 APQ8 MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SC818 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6	c, Snapdrables in A 017, APC 096AU, A 9150, MI 9206, MI 9635M, I 9635M, I 9635M, I 3905, MS 3909W, I 3920, MS 3976, MS 3976, MS 3976, MS 3976, MS 3976, MS 3976, MS 3976, SDM 50, SDM 50, SDM 5150, SDM 545, SDM	ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MDM9655 SM8909, MSM891, SM8953, SM8953, SM8953, SM8953, SM8956, SM8956, SM8956, SM897, S605, Ql 1632, SD 1632, SD 1670, SD 1632, SD 1670, SD 16	9, 8, 6, 7, 40, 6, 47, AU, M215, A845, M450, M636, M710, X20, 150, d_2016  335				
Use After Free	21-11-2019	2.1	daem static freed in Sna Snapo Snapo Snapo Snapo Mobil Music Wear APQ8	fter free on shute object in from a napdragon Caragon Caragon Caragon Indragon Indra	lown dunstance grant properties on sume andustria parties on Vagon APQ800 Q8053,	e to getting places  vity, r IOT, l IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

MDM9150, MDM9206, MDM9206, MDM92070, MDM9650, MSM8905, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8937, MSM8996, MSM8998, Nisher, QCS605, SDA660, SDM450, SDM660, SDM451, SDM24, SM6150, SM6150, SM6150, SM710, SDM845, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	Weakness	Publish Date	cvss	Description & CVE ID	Pato	h	NCIIP	C ID
Improper Validation of Array Index  21-11-2019  Array Shapel Shap				MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130				
	Validation of	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20	w.qualcom.com/pany/pct-securitylletins/ber-201	com /com rodu y/bu octo	MSM8-	/1360

(CVSS)

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	CID
Out-of- bounds Read	21-11-2019	10	while session messar un-information of the session messar un-information of the session messar un-information of the session o	r over reparsing on manage ages if new dragon Adragon Coloragon Indragon In	downlingement etwork stalues in uto, ompute onsume ndustria oT, Snaparagon Vagon APQ800 DM9625 DM9625 DM9625 DM9625 DM9625 DM9625 DM9655 DM8976, SD855 DM568 DM8976, DM9655 DM96	nk OTA sends	https:/w.qualm.company/jct-securitelletins/ber-20bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219,	/1361
Improper Authenticati	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can			https:/ w.qual m.com	com	H-QUA- MSM8-		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	n & CVE	ID	Pat	ch	NCIIP	CID
on			result	into aut	henticat	tion	pany/	produ	031219	/1362
			bypas	s of NAS	in		ct-			
			Snapo	lragon A	uto,		securi	ty/bu		
			Snapo	lragon C	ompute	,	lletins	octo/		
			Snapo	lragon C	onsume	r IOT,	ber-20	19-		
			Snapo	lragon Ir	idustria	l IOT,	bulleti	n		
			^	lragon Io	•	O				
				e, Snapd	_	oice &				
				, Snapdr	•					
				ables in A	•	9,				
			_	017, APC	•	_				
			_	096AU, A	•					
				9150, MI		•				
				9206, MI		•				
				9615, MI						
				9635M, I		•				
				9650, MI						
				3905, MS						
				3909W, N		•				
				3920, MS	•					
				3939, MS	•					
				3953, MS						
				3996AU,		•				
				ar, QCM	. •	•				
			_	.5, SC818		•				
				45, SDM	,	,				
				50, SDM	•	•				
				36, SDM 10, SDM	•	•				
				10, SDM 0, SDX24	•	•				
				•	•	•				
			SM82	50, SM7	150, SM	0130,				
				ou, lragon_H	ligh Mo	d 2016				
			^	130, SXI	•	u_2010				
			·	•						
				D : CVE-			,	, ,		
Improper				nation d			https:/	•		
Restriction				k of addr			w.qual		H-QUA-	
of	21-11-2019	2.1		done on	•		m.com	-	MSM8-	
Operations				s in SDI			pany/	produ	031219	/1363
within the			_	lragon A			ct-	/1.		
Bounds of a			Snapo	lragon C	ompute	, 	securi	ty/bu		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Memory Buffer			Snapo Snapo Snapo Snapo Snapo Infras Netwo APQ8 MDM9 MSM8 MSM8 MSM8 QCS40 SDA6 SDM6 SDM6 SDM6 SDM6 SDM8 Snapo	dragon_F	onsume ndustria Mobile, Yoice & M Vired e and n APQ80 Q8053, SM8905 SM8937, SM8937, SM8953, cobar, Q M205, QM2 1450, SD M450, SD M450, SD M450, SD M450, SD M450, SD M450, SD	r IOT, l IOT, l usic, 09, , CS404, 215, M429, M630, M660, M845,	lletins, ber-20 bulleti	19-		
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM	P modul out side it receiv nessage. Snapdra dragon In dragon Io e, Snapdra shles in Io 9150, MI 9206, MI 9615, MI	its bour res malfo in Snapo agon Cor consume ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9605 DM9605 MDM9625	ndary ormed dragon npute, r IOT, dragon oice &  9, 8, 5, 7, 140,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	/com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1364
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	tch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	3905, MS 3909W, N 3920, MS 3939, MS 3953, MS 3996AU, ar, QCM 55, SC818 45, SDM 45, SDM 50, SDX24 50, SM7 50, dragon_H	MSM8917, SM8940, SM8976, MSM89 2150, Qu 429, SD 429, SD 4660, SD 4660, SD 47, SD 550, SM 4150, SM	98, CS605, A660, M439, M632, M670, M850,				
			CVE I	D : CVE-	2019-2	303				
N/A	21-11-2019	7.2	copy to the Param are from environment of Snapo	e invokin from fd of e secure la neters be om non so onment. Snapdra dragon C dragon I dragon W dragon	or local laboration of local laborations of l	ouffer oulated dragon mpute, vity, or IOT, l IOT, dusic, U,	https:/ w.qual m.com pany/j ct- securif lletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- MSM8- 031219	/1365
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID				Pat	ch	NCIIP	C ID
			MSM8 QCS46 SDA6 SDM6 SDM6 SDM8 SM81 Snapo	lragon_I 1130, SX	MSM89 605, QM2 845, SDM (450, SD (636, SD (710, SD 150, SM High_Me R2130	98, 215, M429, M630, M660, M845, 7150,				
Out-of- bounds Read	21-11-2019	2.1	Trusti memo result Snapo	CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016				//ww com /com produ ty/bu /octo 19- n	H-QUA- MSM8- 031219	/1366
msm8937										
Loop with Unreachable Exit Condition	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop			https://ww w.qualcom m.com/com pp pany/produ		H-QUA- MSM8- 031219	/1367	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3 3-4 4-5 5-6			6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIF	PCID
('Infinite Loop')			in Snapo Snapo Snapo Snapo Snapo Snapo Mobil Musio Wears APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SC818 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SDX58 SM81 Snapo	apdragon Clragon Clragon Idragon Idrag	n Auto, fompute, fonsume adustria oT, Snap dragon Vagon APQ800 DM9607 DM9605 DM9605 DM9605 SM8909, MSM891 SM8953, SM850, SM75250,	r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, M215, A845, M450, M636, M710, X20, 150,	ct- securit lletins ber-20 bulleti	ty/bu /octo )19-		
Use After Free	21-11-2019	2.1	daem static freed in Sna Snapo Snapo Snapo	fter free on shutd object ir from a n apdragon dragon C dragon C dragon C	lown dunstance grantiple n Auto, ompute, onnectivonsume	e to getting places , vity, r IOT,	https://w.qual m.com pany/j ct- securit lletins/ ber-20	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descriptio	on & CVE	ID	Pat	ch	NCIIP	C ID
			Mobil Music Wears APQ8 APQ8 MDM' MDM' MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM8	dragon Idee, Snapdre, Snapdre, Snapdre, Snapdre, APC 096AU, APC 19150, MS 1917, MS 1996, SDA 1996, S	ragon V ragon APQ800 Q8053, APQ809 DM9206 MB905 SM8909 SM8939, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953,	oice &  9,  8,  7,  7,  W,  AU,  CS605,  M450,  M710,  24,  8150,	bulleti	n		
Improper Validation of Array Index	21-11-2019	4.6	Out-o occur to imp array Auto, Electr Snape Snape Snape Snape APQ8 APQ8 APQ8 MDM MDM MSM8 MSM8	f-bounds in came proper values index in Snapdra conics Codragon C dragon Ir dragon W dragon W 009, APC 053, APC 098, MD 9207C, M 9640, MI 3905, MS 3909W, MS	s access ra drive alidation Snapdr gon Coronsume dustria dobile, foice & Marable (28017, 28096A) M9206, M9206, M98937, MSM8937, MSM8937,	can r due n of agon nsumer ity, r IOT, I IOT, U, O7, O7,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1369
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM630, SDM636, SDM60, SDX20  CVE ID : CVE-2019-10503  Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8096AU, APQ8096, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9615, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8906, MSM8909, MSM8906, MSM8909, MSM8906, MSM8909, MSM8906, MSM8906, MSM8908, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDM630, SDM632, SDM630, SDM6450, SDM24, SDM550, SM8150, SM8250, Snapdragon_High_Med_2016	Weakness	Publish Date	cvss		on & CVE	ID	Pat	ch	NCIIP	CID	
Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Conpute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8009, APQ8096AU, APQ8098, MDM9150, MDM9605, MDM9605, MDM9605, MDM9605, MDM9605, MDM9605, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8917, MSM8920, MSM8917, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM870, SDM710, SDM845, SDM850, SDX20, SDX20, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016				QCN7 SDM6	605, SD 30, SDM	A660, SI	)M450,				
while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9650, MDM9655, MDM9655, MDM9655, MDM9655, MSM8909, MSM8976, MSM896AU, MSM8976, MSM896AU, MSM898, Nicobar, QCM215, QCS605, QM215, SC8180X, SDA660, SDA645, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM845, SDM850, SDX20, SDX20, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016				CVE I	D : CVE-	2019-1	0503				
CV Scoring Scale		21-11-2019	10	while session messar un-introduced snaped sn	parsing on manages if neitended with tended with tended with tended with tended with tended in t	downling gement of the etwork strainers in auto, compute consume industria of the etwork strainers and the etwork strainers are the etwork strainers and the etwork strainers are the etwork straine	nk OTA sends ar IOT, I IOT, dragon oice & 9, 8, 5, 40, 5, 40, 6, 7, 40, 6, M439, M632, M670, M850, 8150,	w.qual m.com pany/i ct- securit lletins ber-20	com /com produ ty/bu /octo	MSM8-	/1370
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130		
			CVE ID : CVE-2019-2271		
Improper Authenticati on	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909W, MSM8917, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM630, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MSM8- 031219/1371

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIII	PC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape SDM6 SDM6 SDM6 SDM6 SDM8 Snape , SXR1	lragon_H 130	ress range the System to, code. in uto, ompute onnections on sume dustrial lobile, coice & March 1980, SM8905, SM8905, SM8937, SM8953,	ge sDBG , vity, er IOT, l IOT, Music, 09, , , , CS404, 215, M429, M630, M660, M845, d_2016	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
Out-of- bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,				https://w.qualm.com pany/jct- securifiletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM7 SDX2 SM61 SM82 Snapo , SXR1	096AU, A 9150, MI 9206, MI 9615, MI 9635M, II 9650, MI 3905, MS 3909W, II 3920, MS 3939, MS 3953, MS 3	DM9205 DM9607 DM9625 MDM964 DM9655 GM8909, MSM891 GM8976, GM89	5, 7, 6, 40, 5, 17, 98, CS605, A660, M439, M632, M670, M850, 5,				
N/A	21-11-2019	7.2	copy to the Paran are from environment of Snapo	e invokin from fd of secure lancers be om non sonment. Snapdra dragon C dragon C dragon W dragon W dragon W dragon W dragon W dragon W dragon W dragon W dragon W	or local bouffer, eing popsecure in Snape onnectivonsume dustria foice & March 1998 on	ouffer oulated dragon mpute, vity, or IOT, l IOT, fusic,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130		
Out-of- bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MSM8- 031219/1375

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			CVE I	D : CVE-	2019-2	318				
msm8940	l									
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condification of the condist result in Snaped Snaped Snaped Snaped Snaped Mobil Music Weara APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SDX59 SNaped SNaped SNaped SNaped SNaped SNaped MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM	process messag tion is no ing into apdragon C dragon It dragon, MI dragon, MI dragon, MI dragon, SDM dragon, SDM dragon, SDM dragon, SDM dragon, SDM dragon, SC dragon, S	ge, Valid of met an infin in Auto, ompute onsume industria oT, Snap lagon Vagon APQ800 DM9607 DM9607 DM9607 DM9655 SM8909 MSM8937 SM8953 SM895	exit ite loop , er IOT, l IOT, dragon oice & e9, 8, 5, 7, 5, 40, 5, 17, AU, M215, A845, M450, M636, M710, X20, 150, d_2016	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1376
Use After	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to			https:/	•	H-QUA-		
Free			daem	on shutd	lown du	e to	w.qual	com	MSM8-	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			static freed in Snapo Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wear; APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SM61 SM82 CVE I	object ir from a napdragon Caragon Caragon Ir dragon Ir	astance and tiple and Auto, ompute, onnectivonsume and stria of T, Snap aragon Vagon APQ809 DM9206 MB909 SM8909 SM8939, SM8939, SM8939, SM8953, SM8953, SM8953, SM8953, SM8953, SM8953, SM8956 APQ, SDX SM8956	getting places vity, r IOT, l IOT, dragon oice & 9, 8, 7, W, CS605, M710, 24, 8150,	m.com pany/j ct- securit lletins ber-20 bulleti	produ ty/bu /octo 119-	031219	7/1377
Improper Validation of Array Index	21-11-2019	4.6	occur to imparray Auto, Electr Snapo Snapo Snapo Snapo Snapo APQ8	f-bounds in came proper veindex in Snapdra conics Codragon Celragon Meragon Wergon Wergon Wergon Wergon Wergon Wergon Wergon Wergon Wergon APC	ra drive alidation Snapdra gon Cor onsume ndustria Iobile, Toice & M Vearable Q8017,	r due n of agon isumer ity, r IOT, l IOT, fusic, es in	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> MSM <sup>o</sup> QCN <sup>o</sup> SDM <sup>o</sup> SDX <sup>o</sup>	098, MD 9207C, N 9640, MI 3905, MS 3909W, N 3920, MS 3940, MS 3996AU, 605, SDA 30, SDM 0	MDM960 DM9650 M8909, MSM8937, SM8953, MSM89 A660, SI	07, 0, 17, 98, 0M450,				
Out-of- bounds Read	21-11-2019	10	while session messar un-information of Snapor Snapo	r over reparsing on manages if netended voltagen Collagon Collagon Indicates in August 1965, MI 1965,	downlingement etwork stalues in uto, ompute onsume ndustria oT, Snappragon Vagon APQ800 Q8053, APQ809 DM9607 DM9605 DM9605 DM9605 DM9655 DM965	nk OTA sends  r IOT, dragon oice & 9, 8, 5, 40, 5, 40, 5, 40, 65, 40, 65, 4660,	https:/w.qualm.com pany/jct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1379
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SM8250, SM8250, Snapdragon, High, Med_2016, SXR1130, SXR2130	Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	CID
Allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8093, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9205, MDM9206, MDM9650, MDM9650, MDM9655, MSM8909W, MSM8917, MSM8937, MSM8996AU, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM430, SDM430, SDM430, SDM630, SDM630, SDM630, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDM850, SDM850, SDM845, SDM850, SDM				SDM6 SDM7 SDX2 SM61 SM82 Snapo	36, SDM 10, SDM 0, SDX24 50, SM7 50, dragon_H	660, SD 845, SD 5, SDX55 150, SM High_Me R2130	M670, M850, , 8150, d_2016				
-	Authenticati	21-11-2019	10	allow NAS result bypas Snapo Snapo Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM' MDM' MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4	s MODEI nessages into aut is of NAS dragon A dragon C dragon In dragon Ic dr	M to accident to a	ept any can tion  r IOT, l IOT, dragon foice & 9, 8, 5, 7, 7, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,	w.qual m.com pany/i ct- securit lletins ber-20	ty/bu /octo	MSM8-	/1380
11 (188)	CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Dat	te CVS	5	Description	on & CVE	Pat	tch	NCIIP	CID	
Weakness	Publish Dat	te CVS	SDX2 SM62 SM82 Snap , SXR CVE I Infor to lac checl buffe Snap Snap Snap Snap	20, SDX24 150, SM7 250, dragon_I 1130, SX ID : CVE- mation d ck of addi k done on rs in SDI dragon A dragon C dragon C dragon C	4, SDX55 150, SM High_Me R2130 2019-2 Hisclosur ress rang the Syst code. in Auto, Compute Connective Consume	289 ee due ge sDBG vity, vity, er IOT,	Pat	tch	NCIIP	CID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-201	2.1	Snap Snap Infra Netw APQE MDM MSM MSM QCS4 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6	dragon_I	Voice & M Vired e and n APQ80 Q8053, SM8905 SM8937, SM8953, cobar, QM2 845, SDM 1450, SD 1450, SD 1710, SD	09, , , , , , , , , , , , , , , , , , ,	https://w.qualm.com pany/jct-securifiletins ber-20 bulleti	lcom l/com produ ty/bu /octo	H-QUA- MSM8- 031219	/1381
Out-of- bounds Read	21-11-201	7.5	array wher XID r	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute,			https://w.qualm.com pany/j	lcom 1/com	H-QUA- MSM8- 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	I	Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	lragon Collagon Inagon	ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9607 DM9625 MDM9655 SM8909, MSM891 SM8937, SM8940, SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8937, SM8940, SM8955 SM8955 SM8976, MSM891 SM8976, MSM891 SM8937, SM8	1 IOT, dragon oice & 9, 8, 5, 40, 5, 40, 6, 4660, M439, M632, M670, M850, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	securit lletins, ber-20 bulleti	octo 19-		
N/A	21-11-2019	7.2	copy for to the Param are from t	invoking from fd of secure lands become none somment. Snapdragon Caragon Caragon Inagon Inago	or local bouffer, eing popsecure in Snapelgon Coronnectivons under the consume	ouffer oulated dragon npute, vity, r IOT,	https://w.qual m.com pany/j ct- securit lletins/ ber-20 bulleti	com /com orodu cy/bu /octo 19-	H-QUA- MSM8- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ſ	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Infras Netwo APQ8 APQ8 APQ8 MDM9 MSM8 MSM8 MSM8 MSM8 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SDM8 SM81 Snapo	lragon_H 130, SX	oice & Maried and APQ80 (28053, Q8096A) (28096A)	09, U, 5, 0), 98, 215, M429, M630, M660, M845, 7150,				
Out-of- bounds Read	21-11-2019	2.1	CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920,				https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1384
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 QM21 SDM4 Snapo	3937, MS 3953, MS 3996AU, 15, SDM 350, SDM dragon_F <b>D: CVE-</b>	SM8996, QCA808 129, SDM 1632, High_Me	31, 1439, d_2016				
msm8996			0,2,	2.072						
Use After Free	21-11-2019	2.1	daem static freed in Sna Snapo Snapo Snapo Snapo Snapo Mobil Musio Wear APQ8 APQ8 MDM MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61 SM82	fter free on shutch object in from a map dragon Coloragon Coloragon Idragon Id	down dunstance grant place of Auto, compute connective consume and corrective corrective consume and corrective	e to getting places  vity, r IOT, l IOT, dragon oice &  9,  8,  7,  W,  AU, CS605, M710, 24, 8150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MSM8- 031219	/1385
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer			https:/ w.qual	•	H-QUA- MSM8-		
CV Scoring Scale (CVSS)	e 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6			6-7	7-8	8-9	9-10	

to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096, APQ8096AU, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8906, MSM8937, MSM8998, QC5404, QC5605, QM215, SDA660, SDA845, SDM620, SDM632, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM640, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon, High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Con	Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIF	PCID
are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8990, MSM8917, MSM8990, MSM8917, MSM8990, MSM8917, MSM8996, MSM8995, MSM8998, QCS404, QCS605, QM215, SDA660, SDA945, SDM429, SDM439, SDM450, SDM630, SDM632, SDM630, SDM630, SDM632, SDM630, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon, High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, State Industrial IOT, State Industrial Industrial IOT, Sc				to the	secure l	ouffer,		m.com	/com	031219	/1386
environment. in Snapdragon compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8096, APQ8096AU, APQ8096A, APQ8096AU, APQ8096, MDM9607, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909, MSM8917, MSM8990,				Paran	eters be	eing pop	ulated	pany/j	produ		
Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8093, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8990, MSM8917, MSM8990, MSM8917, MSM8990, MSM8917, MSM8990, MSM8917, MSM8990, MSM8917, MSM8990, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8998, QC\$404, QC\$605, QM215, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM630, SDM670, SDM710, SDM845, SDM630, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Consumer IOT, Snapdragon Industrial IOT.  CV Scoring Scale  1.1 23 33 34 45 56 67 78 88 9 10				are fro	om non s	secure		ct-			
Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8093, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8937, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA650, SDM630, SDM632, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SD						•	O	securit	y/bu		
Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8093, APQ8096, APQ8096AU, APQ8096, MDM9205, MDM9206, MDM9607, MDM9205, MSM8909, MSM8917, MSM8920, MSM8907, MSM8907, MSM8909, MSM8917, MSM8920, MSM8937, MSM8996, MSM8996AU, MSM8937, MSM8996, MSM8996AU, MSM8937, MSM8998, QCS404, QCS605, QM215, SDA660, SDA645, SDM429, SDM439, SDM430, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016				·	•	U	•	•			
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, MSM8953, MSM8996, MSM8953, MSM8998, QCS404, QCS605, QM215, SDA660, SDM630, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IOT, Sna				Snapd	lragon C	onnectiv	vity,				
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, MSM8940, MSM8937, MSM8940, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 ,SXR1130, SXR2130 CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  Out-of- bounds Read				^	•			bulleti	n		
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, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM630, SDM630, SDM632, SDM660, SDM6710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 ,SXR1130, SXR2130 CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Security/bu Iletins/octo Snapdragon Industrial IOT, Der-2019-  CV Scoring Scale  Out-of- bounds Read				_			l IOT,				
Snapdragon Wired   Infrastructure and   Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096, APQ8096, APQ8096, MDM9150, MDM9206, MDM9206, MDM9206, MDM9650, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8937, MSM8996, MSM896AU, MSM8953, MSM8996, MSM896AU, MSM8953, MSM8996, MSM896AU, MSM8953, MSM8998, QCS404, QCS605, QM215, SDA660, SDM670, SDM450, SDM630, SDM632, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130				_	Ū						
Infrastructure and   Networking in APQ8009,   APQ8017, APQ8017, APQ8053,   APQ8096, APQ8096, APQ8096, APQ8096, APQ8096, MDM9150,   MDM9205, MDM9206,   MDM9205, MDM9206,   MDM9607, MDM9206,   MDM9607, MDM9650,   MSM8905, MSM8909,   MSM8917, MSM8920,   MSM8997, MSM89940,   MSM8996,   MSM8998,   QCS404, QCS605, QM215,   SDM630, SDM630, SDM630, SDM632, SDM630, SDM6450, SDM6450, SDM6450, SDM6450, SDM710, SDM845,   SDM850, SM6150, SM7150,   SM8150, SM8150, Smaptragon_High_Med_2016, SXR1130, SXR2130   CVE ID : CVE-2019-2315				_	Ū		Iusic,				
Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096, APQ8096AU, APQ8096, APQ8096AU, APQ8096, MDM9150, MDM9206, MDM9607, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8909, MSM8917, MSM8920, MSM8997, MSM8996, MSM8996, MSM8996, MSM8996, MSM8996, MSM8996, MSM8996, MSM8996, MSM8998, QCS404, QCS605, QM215, SDA660, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2315    Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Connectivity, Snapdragon Industrial IOT, ber-2019-				^	•						
APQ8017, APQ8053,											
APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8937, MSM8996, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  0.1 1.2 23 3.4 4.5 5.6 6.7 7.8 8.9 8.10					O	•	09,				
APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  APQ8098, MDM9150, MDM9205, MDM9206, MDM9205, MDM9206, MSM89909, MSM8991, MSM8998, QCS404, QCS605, QM215, SDM630, SDM630, SDM632, SDM630, SDM632, SDM630, SDM630, SDM630, SDM632, SDM640, SDM630, SDM640, SNR150, SNR1130, SXR2130  CVE ID: CVE-2019-2315  H-QUA- MSM8- 031219/1387				_		•					
MDM9205, MDM9206, MDM9650, MDM9650, MSM8905, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8996AU, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDM439, SDM450, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon In				_		•					
MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA645, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  Out-of- bounds Read				_ ~	•	-					
MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  0.1 1.2 2.3 3.4 4.5 5.6 6.7 7.8 8.9 8.10											
MSM8917, MSM8920, MSM8937, MSM8940, MSM8937, MSM8996, MSM8996, MSM8996, MSM8996, MSM8996, MSM8996, MSM8996, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130											
MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID: CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  Out-of- bounds Read  MSM8- 031219/1387					•	•					
MSM8953, MSM8996,   MSM8998,   QC\$404, QC\$605, QM215,   SDA660, SDA845, SDM429,   SDM439, SDM450, SDM630,   SDM632, SDM636, SDM660,   SDM670, SDM710, SDM845,   SDM850, SM6150, SM7150,   Smapdragon_High_Med_2016   , SXR1130, SXR2130					•	•					
MSM8996AU, MSM8998,   QCS404, QCS605, QM215,   SDA660, SDA845, SDM429,   SDM439, SDM450, SDM630,   SDM632, SDM636, SDM660,   SDM670, SDM710, SDM845,   SDM850, SM6150, SM7150,   SM8150,   Snapdragon_High_Med_2016   , SXR1130, SXR2130					-	•					
Out-of-bounds Read  Out-of											
Out-of-bounds Read  Out-of					•		•				
SDM439, SDM450, SDM630, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Socie CV Scoring Scale CV S				_							
Out-of-bounds Read  Out-of											
Out-of-bounds Read  Out-of					•	•	•				
SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  Out-of- bounds Read  21-11-2019  CV Scoring Scale  Out-of- bounds Read  Out-of- Double Read  Out-o				SDM6	70, SDM	710, SD	M845,				
Snapdragon_High_Med_2016 , SXR1130, SXR2130  CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  O-1  1-2  2-3  3-4  4-5  5-6  6-7  7-8  8-9  9-10				SDM8	50, SM6	150, SM	7150,				
Out-of-bounds Read  21-11-2019  2.1  Out-of-bounds Read  Out-of-bo				SM81	50,						
Out-of-bounds Read  21-11-2019  2.1  Out-of-bounds Read  CVE ID : CVE-2019-2315  Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Scale  CV Scoring Scale  Out-of-bounds Read  CVE ID : CVE-2019-2315  Non Secure Kernel can cause https://ww w.qualcom m.com/com pany/produ ct-security/bu Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Industrial				Snapd	lragon_H	ligh_Me	d_2016				
Out-of-bounds Read  21-11-2019  Anon Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT,  CV Scoring Scale  O-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				, SXR1	130, SX	R2130					
Out-of-bounds Read  21-11-2019  2.1  Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  O-1  1-2  2-3  3-4  4-5  5-6  6-7  7-8  8-9  9-10				CVE I	D : CVE-	2019-2	315				
Out-of-bounds Read  21-11-2019  2.1  Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  O-1  1-2  2-3  3-4  4-5  5-6  6-7  7-8  8-9  9-10				Non S	ecure Ke	ernel car	n cause	https:/	//ww		
Out-of-bounds Read  21-11-2019  2.1  memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  O-1  1-2  2.1  memory read which will m.com/com pany/produ ct-security/bu Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,  CV Scoring Scale  O-1  1-2  2-3  3-4  4-5  5-6  6-7  7-8  8-9  9-10				Trustz	zone to d	do an arl	bitrary	• •	•		
Out-of-bounds Read  21-11-2019  2.1 result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IOT, Industrial IOT, Sn							•	•		Н-ОПА	
Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IOT, Industrial IOT, Industri	Out-of-	21-11-2019	2.1		_				-	_	-
Snapdragon Connectivity, security/bu lletins/octo lletins/octo ber-2019-	bounds Read	21 11 2017	2.1	Snapd	lragon A	uto,		ct-			/1387
Snapdragon Industrial IOT, ber-2019-  CV Scoring Scale  0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				Snapd	lragon C	onnectiv	vity,	securit	y/bu	001217	, , 1307
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				Snapd	lragon C	onsume	r IOT,	lletins	octo/		
1 1-1 1-1 1-2 1 2-3 1 3-4 1 4-5 1 5-6 1 6-7 1 7-8 1 8-9 1 9-111				Snapd	lragon Ir	ndustria	l IOT,	ber-20	19-		
	CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8953, MSM8996, MSM896AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318	bulletin	
sdm450					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM4- 031219/1388

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

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, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM4- 031219/1389

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SM82	50, SXR2	2130					
			CVE I	D : CVE-	2019-1	0490				
Improper Validation of Array Index	21-11-2019	4.6	occur to imparray Auto, Electr Snapo Snapo Snapo Snapo APQ8 APQ8 APQ8 MDM' MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDX2	f-boundin came proper vindex in Snapdra conics Coloragon Magon Vinagon	ra drive alidation Snapdr igon Cor onnectiv consume idustria Mobile, Yearable Q8017, Q8096A M9206, M9206, MM960 DM9650 SM8937, SM8937, MSM89 MSM8937, MSM89 MSM8937,	r due n of agon nsumer ity, r IOT, l IOT, U, 07, 07, 07, 08, 0M450, M660,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Out-of- bounds Read	21-11-2019	10	while session messa un-int Snapo Snapo Snapo Snapo Snapo Mobil Musio	parsing parsing manages if ne tended valued tragon Caragon Indragon Indrago	downlingement of the setwork straines in the setwork straines of the setwork s	nk OTA eends  r IOT, I IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal	e o	1.3			-		c =	7.0		0.40
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			APQ80 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 Nicoba QM21! SDA84 SDM4! SDM63 SDM72 SDX20 SM615 SM825 Snapdi	150, Mi 206, Mi 206, Mi 2635M, I 2635M, I 2650, Mi 905, MS 909W, I 920, MS 939, MS 953, MS 954, SDM 955, SDM 956, SDM 95	APQ809 DM9205 DM9607 DM9625 MDM9655 MSM8909 MSM8937 SM8940 SM8976 MSM8976 MSM89 2150, Q 80X, SD 429, SD 1660, SD 1660, SD 1845, SD 150, SM	5, 7, 6, 40, 5, 17, 98, CS605, A660, M439, M632, M670, M850, 5,				
Improper Authenticati on	21-11-2019	10	allows NAS m result bypass Snapdi Snapdi Snapdi Snapdi Mobile Music, Weara APQ80	e MODEN lessages into aut s of NAS ragon A ragon C ragon Io ragon Io e, Snapd Snapdr bles in 2 017, APO	outo, compute consume ndustria oT, Snap lragon V ragon APQ800	ept any can tion  or IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch:	NCIIP	CID
			MDM MDM MSM8 MSM8 MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR2	9206, MI 9615, MI 9635M, I 9650, MI 3905, MS 3909W, I 3920, MS 3939, MS 3953, MS 3996AU, bar, QCMI 55, SC818 45, SDM 45, SDM 45, SDM 710, SDM 710, SDM 710, SDM 710, SM7 50, SM7 50, SM7	DM9625 MDM9655 MB909, MSM8915 SM8937, SM8976, MSM89 2150, Q0 30X, SDA 429, SDA 429, SDA 5660, SD 6660, SD 6845, SD	5, 40, 5, 17, 98, CS605, A660, M439, M632, M670, M850, 5,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape Snape Snape Snape Snape Snape Snape Snape Snape Model MSM8 MSM8	mation d k of addr done on rs in SDI dragon C dragon C dragon Ir dragon Ir dragon W dragon W structure orking in 017, APO 9205, MS	ress range the System the System to the Syst	ge sDBG  vity, or IOT, l IOT, fusic,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			QCS4 SDA6 SDM6 SDM6 SDM6 SDM8 Snapo	MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130  CVE ID: CVE-2019-2295  SNDCP module may access						
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	P modulout side it received ressage. Snapdra dragon Idragon Id	its bounces malfing Snaper Gonsume and Stragon Varagon	ndary ormed dragon mpute, er IOT, el I	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA-3 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness N/A	Publish Date  21-11-2019	7.2	SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130  CVE ID: CVE-2019-2303  While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8905, MSM8909, MSM8917, MSM8920,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-	H-QUA-SDM4- 031219/1395
			MSM8905, MSM8909,	,	

4-5

6-7

7-8

5-6

9-10

8-9

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM896AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4- 031219/1396
sm8250					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SM82- 031219/1397

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MDM <sup>4</sup> MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM4 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9615, M. 9635M, E. 9635M, E. 9650, M. 8905, M. 8909W, I. 8920, M. 8940, M. 8976, M. 8998, Nic. 2150, Q. 80X, SD. 845, SM. 845, SD.	MDM9655 M8909, MSM8937, SM8953, SM8956, cobar, S605, Q 1632, SD 1632, SD 1670, SD 1650, SM7 250, High_Me R2130	M215, AU, M215, A845, M450, M636, M710, X20, 150, d_2016				
Use After Free	21-11-2019	2.1	daem static freed in Sna Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MSM8	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920,				//ww .com ./com produ ty/bu /octo 119- n	H-QUA-: 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	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, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130		
			<b>CVE ID : CVE-2019-10490</b> Buffer overflow can occur in		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID: CVE-2019-10566	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SM82- 031219/1399
Buffer Copy without Checking Size of Input ('Classic Buffer	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in	https://ww w.qualcom m.com/com pany/produ ct- security/bu	H-QUA-SM82- 031219/1400
CV Scoring Scale (CVSS)	e 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Overflow')			Snapo Snapo Snapo Snapo Snapo Snapo Snapo APQ8 MSM8 Nicob SA61! SDA8 SDM6 SDM6 SM61 SM82	dragon Adragon Colragon Colragon Colragon Maragon Mara	ompute onnective onsume onsume dobile, foice & M Q8096A M9205, MSM89 405, QCS 180X, SI 1670, SD 1670, SD 150, SM	vity, er ity, er IOT, l IOT, Music in U, 98, 605, DA660, M636, M710, X24, 8150, KR2130	lletins, ber-20 bulleti	19-		
Out-of- bounds Read	21-11-2019	10	while session messar un-information Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM	Buffer over read can happen while parsing downlink session management OTA messages 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, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,		https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-3		
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch.	NCIIP	C ID
			MSM8 MSM8 MSM8 Nicob QM21 SDA8 SDM6 SDM7 SDX2 SM61 SM82 Snapo	3909W, I 3920, MS 3939, MS 3953, MS 3996AU, ar, QCM 55, SC818 45, SDM 50, SDM 710, SDM 710, SDM 750, SM7 50, dragon_H 1130, SX	5M8937, 5M8940, 5M8976, MSM89 2150, Q0 30X, SDA 429, SDI 6630, SD 6660, SD 845, SD 845, SD 150, SM	98, CS605, A660, M439, M632, M670, M850, ,,				
Improper Authenticati on	21-11-2019	10	Lack of allow NAS result bypas Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MSM8 MSM8	of integris MODEN nessages into aut is of NAS dragon A dragon C dragon In dragon Ic dragon Ic dragon Ic 3, Snapdr ables in A 9150, MI 9206, MI 9635M, I 9635M, I 9635M, I 89630, MS	ity check M to accombined to chentical in uto, ompute onsume ot, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9625 MDM9645 SM8909, MSM891	ept any can tion  r IOT, l IOT, dragon oice &  9,  8,  7,  40,  5,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2289 SNDCP module may access							
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modul out side it receiv lessage. E Snapdra dragon Ir dragon Ir dragon Ir s, Snapdra dolf, Snapdra 2017, APC 096AU, A 9150, MI 9615, MI 9635M, I 9635M, I 9635M, I 9635M, I 8905, MS 8909W, I 8909W, I 8939, MS	its bountes malfolin Snapolis gon Coronsume adustria oT, Snapolis ragon APQ800 Q8053, APQ809 DM9605 DM9605 DM9605 DM9605 DM9605 DM9655 DM8940, BM8937, BM8940, BM8940	ndary ormed dragon npute, r IOT, dragon oice & 9, 8, 5, 40, 5, 47, 47, CS605, A660,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-: 031219	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID: CVE-2019-2303		
sxr2130					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8917, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR2- 031219/1404

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID: CVE-2019-2336	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SXR2- 031219/1405
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SXR2- 031219/1406
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SXR1	130, SXR	R2130					
			CVE I	D : CVE-	2019-2	339				
Use After Free	21-11-2019	2.1	daem static freed in Sna Snapo Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 APQ8 MDM MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SM61 SM82	tter free on shutch object in from a managem of the degree	down dunstance grultiple in Auto, sompute sonnective on Sume and stria oT, Snap dragon Vagon APQ800 Q8053, APQ809 GM8905 GM8905 GM8905 GM8939,	e to getting places , vity, or IOT, l IOT, dragon oice & 9, 8, 5, 07, , W, CS605, M450, M710, 24, 8150,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Buffer Copy				r overflo			https:/	•		
without Checking Size of Input ('Classic	21-11-2019	4.6	rates eleme than r	module : or exten ent lengt nax rate lragon A	ded rate h is grea set leng	es iter	w.qual m.com pany/j ct- securit	/com produ	H-QUA- 031219	
Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer				lletins/octo ber-2019-			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7 7-8		8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			Snapo Snapo Snapo APQ8 APQ8 MDM9 MSM8 QCA6 QCA9 QCN7 SDA8 SDM8	ronics Co dragon D dragon M dragon V 017, APO 096AU, 9207C, M 3996AU, 174A, Q 377, QC, 605, QC 45, SDM 45, SDM	Consumendustriandustri	er IOT, al IOT, Music in 06, 07, 6, AU, CS605, M710, 150,	bulleti	n		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bir from a source that the potent buffer Snape Sn	tmap file any un-a e, there he bitma tially ca r overflo dragon A dragon A dragon B dragon B	e is load authenti is a poss ap can use staction. In auto, compute connective consumerations and autorial dobile, autorial do	ed cated sibility k  , vity, er ity, er IOT, al IOT, U, 98, 605, DA660, M636, M710, X24,	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-: 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	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-2019-2251		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8909, MSM8917, MSM8939, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, MSM8953, MSM8940, SDM630, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM630, SDM6	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	
CV Scoring Scal	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

(CVSS)

Weakness	Publish Date	CVSS	ſ	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Improper Authenticati on	21-11-2019	10	allows NAS n result bypas Snape Snape Snape Snape Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	of integrals MODEI nessages into autors of NAS dragon A dragon College of Snapdrables in 2017, APO 1096AU, A 1096AU,	M to acc s which a chentical in uto, ompute onsume industrial oT, Snap ragon APQ800 Q8053, APQ809 DM9605 DM9625 DM9625 DM9625 DM9625 DM9635 SM8940, SM8937, SM8940, SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM891 SM8976, MSM8937, SM8976, MSM891 SM891 SM	ept any can tion  for IOT, l IOT, dragon foice & 9, 8, 5, 7, 6, 40, 5, 4660, M439, M632, M670, M850, 6, 8150, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Out-of- bounds Read	21-11-2019	7.5	array	P modul out side	its bour	ndary	https:/ w.qual	com	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	it receiv	4-5	5-6	m.com	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	CID
TO CURITIESS			XID m Auto, Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	nessage. in Snapdra dragon Coloragon Indragon In	in Snapo gon Con onsume dustria oT, Snap ragon APQ800 Q8053, APQ809 DM9607 DM9625 MDM9645 SM8909, MSM891 SM8937, SM8940, SM8976, MSM891 SM8976, MSM8976, MSM891 SM891 SM	dragon inpute, r IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 40, 6, M439, M632, M670, M850, M850, 1, 8150, d_2016	pany/j ct- securit lletins ber-20 bulleti	produ ty/bu /octo 119-	, veni	
N/A	21-11-2019	7.2	While copy to the Param are freenviro Auto,	D: CVE- e invokin from fd of e secure le neters be om non s onment. Snapdra dragon C	g the AP or local to ouffer, eing pop secure in Snapo	PI to ouffer oulated dragon npute,	https://w.qualm.com pany/jct- securit lletins, ber-20	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Snapo Snapo Snapo Infras Netwo APQ8 APQ8 APQ8 MDM MSM8 MSM8 MSM8 MSM8 SDA6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SM81 Snapo	dragon C dragon Indragon Willington Willington Willington Willington Willington Millington Millingt	ndustria Mobile, Moice & M Vired and APQ80 Q8053, Q8096A M9150, DM9206 DM9650 SM8920, SM8940, SM8940, SM8940, SM8940, MSM89 MSM896, MS	l IOT,  fusic,  fusic,	bulleti	n		
Use After Free	21-11-2019	7.2	cleand missing for a fapplic Comp Consu Indus Mobil Infras Netwood QCS40 SDM6	ter free up routing pointer failed station. in the cation of the cation	ne due to er saniti ort of a to orthogon of Snapdo orthogon V erand orthogon orthogo	zation rusted ragon ragon ragon Vired 205, 845,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			SM81	50, SXR	1130, SX	R2130				
			CVE I	D : CVE-	2019-2	329				
apq8016							l			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	from source that to potent buffer Snape Sn	tmap file any un-a e, there he bitma r overflo dragon A dragon C dragon C dragon C dragon I dragon I dragon I dragon V 016, APC 098, MD 3996AU, bar, QCS4 55P, SC8 45, SDM 660, SDM 50, SM7 50, SM7	is a possip can use stack w. in auto, compute, connective consume adustria Mobile, Mos	cated dibility k  k  vity, r ity, r ity, l IOT, l I	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•
sa6155p							T			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,				https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7 7-8		8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Electric Snapo Snapo Snapo APQ8 APQ8 MSM8 Nicob SA611 SDA8 SDM6 SDM6 SM61	dragon Conics Co	onnective onsume ndustria Mobile, Moice & M Q8096A M9205, MSM89 MO5, QCS 180X, SI 1670, SD 1850, SD	ity, r IOT, l IOT, fusic in U, 98, 605, DA660, M636, M710, X24, 8150,				
			CVE I	D : CVE-	2019-2	251				
sc8180x	T		****			,	ı			
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condition result in Snape Snape Snape Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MDM MDM MDM MSM8 MSM8	e process t messag tion is no cing into apdragon dragon C dragon I dragon I	ge, Valid ot met an infin Auto, ompute onsume of the consume of th	exit ite loop  r IOT, l IOT, dragon oice &  9,  8,  7,  6,  40,  6,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2335		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID: CVE-2019-2251	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SC81- 031219/1418
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
Out-of- bounds Read	21-11-2019	10	while session messar un-information of the session messar un-information of the session messar un-information of the session o	cover reparsing on manages if new tended with the tended with	downlingement etwork stalues in uto, ompute onsume industria oT, Snapuragon Vagon APQ800 DM9625 DM9625 DM9625 DM9625 DM9635 GM8909, MSM8937, GM8940, GM8976, MSM8940, GM8976,	nk OTA sends  , or IOT, ol IOT, oldragon olice & olice	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
Improper Authenticati	21-11-2019	10	allow	of integr s MODEI nessages	M to acc	ept any	https:/ w.qual m.com	com	H-QUA- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch	NCIIF	PC ID
on			result	into aut	hentica	tion	pany/j	produ		
			bypas	s of NAS	in		ct-			
			Snapo	lragon A	uto,		securit	ty/bu		
			Snapo	lragon C	ompute	,	lletins	octo/		
			Snapo	lragon C	onsume	r IOT,	ber-20	19-		
			Snapo	lragon Ir	ndustria	l IOT,	bulleti	n		
			Snapo	lragon Io	T, Snap	dragon				
			Mobil	e, Snapd	ragon V	oice &				
			Music	, Snapdr	agon					
			Weara	ables in A	APQ800	9,				
			APQ8	017, AP0	Q8053,					
			APQ8	096AU,	APQ809	8,				
			MDM	9150, MI	DM9205	, ),				
				9206, MI		•				
			MDM	9615, MI	DM9625	, ),				
			MDM	9635M, I	MDM96	40,				
			MDM	9650, MI	DM9655	, ),				
			MSM8	3905, MS	M8909,					
			MSM8	3909W, I	MSM891	7,				
			MSM8	3920, MS	M8937,					
				3939, MS	•					
			MSM8953, MSM8976,							
				3996AU,		•				
				ar, QCM						
			•	.5, SC818		•				
				45, SDM	•	•				
				50, SDM	•	•				
				36, SDM	•	•				
				10, SDM	•	•				
				0, SDX24	•	•				
				50, SM7	150, SM	8150,				
			SM82	•						
			-	lragon_F	_	d_2016				
			, SXR1	[130, SX]	R2130					
			CVE I	D : CVE-	2019-2	289				
			SNDC	P modul	e may a	ccess	https:/	//ww		
			array	out side	its bour	ndary	w.qual	com		
Out-of-	21-11-2019	7.5	when	n it receives malformed   m.com/co			/com	H-QUA-		
bounds Read	21 11 2017	7.3	XID message. in Snapdragon					produ	031219	)/1421
			Auto, Snapdragon Compute,							
			Snapo	lragon C	onsume	r IOT,	securit	ty/bu		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Snapo Mobil Music Wears APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDA8 SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	dragon Indragon Indra	oT, Snap lragon V ragon APQ800 Q8053, APQ809 DM9607 DM9625 MDM9655 SM8909, MSM8937, SM8940, SM8940, SM8976, MSM8937, SM8940, SM8976, MSM8937, SM8940, SM8976, MSM8937, SM8940, SM8976, MSM8937, SM8940, SM8937, SM8937, SM8940, SM8937, SM8940, SM8937, SM8940, SM8937, SM8930, SM890, SM8900, SM8900, SM8900, SM8900, SM8900, SM8900, SM8900, SM8900,	odragon oice & 19, 18, 5, 40, 5, 17, 6, 17, 6, 18, 18, 198,	lletins, ber-20 bulleti	19-		
sdm850										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi result in Sna Snapo Snapo Snapo	e process t messag tion is n cing into apdragon dragon C dragon I dragon I	ge, Valid ot met an infin n Auto, Compute Consume ndustria	exit ite loop , er IOT, ll IOT,	https:/ w.qual m.com pany/p ct- securit lletins, ber-20 bulleti	com /com orodu cy/bu /octo 19-	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7 7-8		8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Mobil Music Wears APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SC818 SDM4 SDM6 SDM6 SDM6 SDM6 SDM8 SDX5s	e, Snapdrables in 2017, APC 096AU, 29150, MI 9635M, I 9635M, I 9635M, I 8905, MS 8909W, I 8998, Nick 29, SDM 630, SDM 645, SDM 64	lragon V ragon APQ800 Q8053, APQ809 DM9607 DM9605 DM9655 MB9605, MSM8937, SM8953, SM89	Toice &  19,  8,  7,  5,  40,  6,  17,  AU,  M215,  A845,  M450,  M636,  M710,  X20,  150,  d_2016				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	lack of array image Snapo Snapo Snapo Snapo Snapo Snapo Snapo Snapo Netwo	f bound a of check of size whi de elf segn dragon C dragon C dragon I dragon M dragon W structure orking in	of whilted ile readinents. in auto, computed consumendustriando ile, which is and modern mode	elist ng the , vity, er IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130		
			CVE ID: CVE-2019-2339		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID: CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8- 031219/1424
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM8- 031219/1425
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Mobil Music Wears APQ8 APQ8 MDM' MDM' MDM' MDM' MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo	dragon Ide, Snapda e, Snapda c, Snapda o17, APO 096AU, A 9150, Mi 9615, Mi 9635M, Ide 9650, Mi 8905, MS 8909W, Ide 8939, MS 8939, MS 8939, MS 8939, MS 8953,	lragon V ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MDM9655 SM8940, SM8937, SM8940, SM8937, SM8940, SM8937, SM8940, SM8955 150, SD 1630, SD 1630, SD 1630, SD 1630, SD 1630, SD 1630, SD 1630, SD 1630, SD	oice & 9, 8, 5, 7, 5, 40, 5, 4660, M439, M632, M670, M850, 5, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,				
Improper Authenticati on	21-11-2019	10	allow NAS result bypas Snapo Snapo Snapo Snapo Snapo Mobil	of integros MODEl nessages into autors of NAS dragon A dragon C dragon Indragon Indr	M to acc s which chentica in auto, ompute onsume ndustria oT, Snap	ept any can tion , er IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo , SXR1	ables in A 017, APO 096AU, A 9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 3905, MS 3905, MS 3905, MS 3905, MS 3953, MS 3953, MS 3953, MS 3953, MS 3953, MS 3053, MS 3	APQ800 Q8053, APQ809 DM9205 DM9607 DM9625 MDM9655 SM8909, MSM891 SM8937, SM8940, SM8937, SM8940, SM8937, SM8940, SM8937, SM8955 SM8955 SM8976, MSM89 EMBERT SM89 SM8976, MSM89 SM8937, SM8937, SM8937, SM8940, SM8937,	9, 8, 5, 40, 5, 40, 5, 40, 5, 40, 67, M632, M632, M670, M850, 6, 8150,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	to lack check buffer Snape	nation d k of addr done on rs in SDI dragon C dragon C dragon C dragon V dragon V dragon W structure orking in	ress range the System the System to the Syst	ge DBG vity, r IOT, l IOT,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Descriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 MSM8 QCS40 SDA6 SDM6 SDM6 SDM8 Snapo	lragon_H	5M8917, 5M8937, 5M8953, 5obar, Q 505, QM2 6450, SD 6450, SD 636, SD 6710, SD	CS404, 215, M429, M630, M660, M845,				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modulout side it receives age. It sages ages ages ages ages ages ages age	its bountes malformands trian Snapor Corsume adustria oT, Snapor APQ800 Q8053, APQ809 DM9605	ndary ormed dragon npute, or IOT, l IOT, dragon oice & 9, 8, 5, 40, 5, 47, 67, 28, CS605, A660,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-3	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR2	dragon_H 1130, SX <b>D : CVE-</b>	660, SD 845, SD 5, SDX55 150, SM ligh_Me R2130 <b>2019-2</b>	M670, M850, 8150, d_2016				
N/A	21-11-2019	7.2	copy to the Paramare frenvire Auto, Snape	e invoking from fd of a secure lands on none soment. Snapdradragon Caragon Indragon Varagon Varagon, APO 19205, MS 1937, MS 193	or local louffer, eing popsecure in Snapegon Coronsumendustria lobile, oice & Marie and APQ80 (28053, Q8096A (28096A (	ouffer oulated dragon npute, vity, er IOT, l IOT, Usic, 09, U, 5, 0, 4, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,	https:/w.qualm.company/jct-securitilletins/ber-20	ty/bu /octo	H-QUA- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			_	lragon_I I 130, SX	Ū	d_2016				
			CVE I	D : CVE-	2019-2	315				
mdm915										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	Reject condi result in Sna Snapo Snapo Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 SC818 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6 SDM6	process t messag tion is n ing into apdragon of dragon o	ge, Valid ot met an infin in Auto, compute on Sume industria oT, Snap largon Vagon APQ809 DM9607 DM9607 DM9605 SM8909, MSM891 SM8953,	exit ite loop , r IOT, l IOT, dragon oice &  9,  8, , , , , , , , , , , , , , , , ,	https:/ w.qual m.com pany/i ct- securii lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	/1430
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Out-of- bounds Read	21-11-2019	10	while session messar un-interest of the session messar un-interest of snaped Snaped Snaped Snaped Mobil Musico Weara APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 SDM8 SDM8 SDM8	cover reparsing on manage sended valuagion A dragon A dragon I dragon, MI dragon, SDX dragon, SDX dragon, SDX dragon, SDX dragon, SDX dragon, SDX dragon, SX dragon, S	downlingement of tworks alues in uto, ompute onsume industria of, Snap ragon Vagon APQ800 Q8053, APQ809 DM9625 DM9625 DM9625 DM9655 DM8976, SD855 DM568, SD855 DM568, SD855 DM568, SD855 DM568, SD855 DM568 DM968 DM9	nk OTA sends  , or IOT, ol IOT, oldragon olice & olice	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- MDM9- 031219	/1431
Improper Authenticati	21-11-2019	10	allow	of integri s MODEN nessages	M to acc	ept any	https:/ w.qual m.com	com	H-QUA- MDM9-	
CV Scoring Scal	e 0-1	1-2	2-3	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	D	escriptio	n & CVE	ID	Pat	ch	NCIIP	C ID
on			result	into aut	henticat	tion	pany/	orodu	031219	/1432
			bypass	of NAS	in		ct-			
			_	ragon A			securi			
			_	ragon Co	•		lletins			
			_	ragon Co			ber-20			
			_	ragon In			bulleti	n		
			-	ragon Io	•	O				
				e, Snapdi	_	oice &				
				Snapdr	•	_				
				bles in A	•	9,				
			•	17, APÇ						
			•	96AU, <i>A</i>	•					
				150, MI		•				
				206, MI		•				
				615, MI		•				
				635M, N		,				
				650, MI						
				905, MS						
				909W, N		•				
				920, MS	•					
				939, MS 953, MS	•					
				993, M3 996AU, 1	•					
				ır, QCM2		•				
				5, SC818						
			•	5, SCO16						
				50, SDM	•	•				
				36, SDM	•	•				
				LO, SDM	•	•				
				, SDX24	•	•				
				50, SM71	•	•				
			SM825		130, 3141	0150,				
				ragon_H	igh Me	d 2016				
			-	130, SXI	_	u_2010				
				) : CVE-2		280				
qcm2150			GVETE	, GVE						
Loop with			While	le processing Attach https://ww				//ww		
Unreachable	04 44 0040	_		•	•		w.qual	•	H-QUA-	
Exit	21-11-2019	5	QUI				QCM2-	/4.400		
Condition		resulting into an infinite loop pany/produ 031219/12						/1433		
C)/ Cooming = C : 1										
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
('Infinite Loop')			Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM9 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SC818 SC818 SDM6 SDM6 SDM6 SDM6 SDM6 SDM8 SDX58 SM81 Snapo , SXR1	apdragon C dragon C dragon In dragon Io dragon Io e, Snapdr ables in A 017, APO 096AU, A 9150, MI 9615, MI 9635M, I 9635M, I 963M, I 963M, I 963M, I 963M, I	ompute, onsume adustria oT, Snap lagon Vagon APQ800 Q8053, APQ809 DM9605 SM8909, MSM891 SM8953, SM8953, SM8953, S605, Qlaso, SD l632, SD l	r IOT, dragon foice & 9, 8, 5, 7, 40, 5, 40, 6, M215, M450, M636, M710, X20, 150, d_2016	ct- securit lletins, ber-20 bulleti	octo 19-		
Out-of- bounds Read	21-11-2019	10	while session messa un-int Snapo Snapo Snapo	r over re parsing on manag ages if ne tended v dragon A dragon C dragon I	downlir gement ( etwork s ralues in auto, ompute, onsume	nk OTA eends r IOT,	https://w.qual m.com pany/j ct- securit lletins ber-20	com /com produ ty/bu /octo	H-QUA- QCM2- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	ſ	Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			Mobil Music Wears APQ8 APQ8 MDM9 MDM9 MDM9 MDM9 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 MSM8 SDM4 SDM4 SDM4 SDM6 SDM7 SDX20 SM61 SM82 Snapo	Iragon Ide, Snapdon, Snapdon, Snapdon, APO 17, APO 196, MI 196, MI 196, MI 196, MI 196, SDM 10, SDM 10	lragon V ragon APQ800 Q8053, APQ809 DM9205 DM9625 MDM9625 MDM9655 SM8940, SM8937, SM8940, SM8937, SM8940, SM8976, MSM89 2150, Q 80X, SD, 429, SD, 1630, SD, 1630, SD, 1845, SD, 1845, SD, 1845, SD,	oice & 9, 8, 5, 7, 5, 40, 5, 4660, M439, M632, M670, M850, 5, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	bulleti	n		
Improper Authenticati on	21-11-2019	10	allows NAS n result bypas Snapo Snapo Snapo Snapo Snapo Mobil	of integra s MODEI nessages into aut s of NAS lragon A lragon C lragon I lragon I ge, Snapd	M to acc s which thentica in outo, ompute onsume ndustria oT, Snap	ept any can tion , er IOT, l IOT,	https://w.qualm.com pany/jct- securit lletins/ ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- QCM2- 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID
			Wears APQ8 APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	ables in 2 017, APC 096AU, 2 9150, MI 9206, MI 9615, MI 9635M, I 9635M, I 3905, MS 3905, MS 3905, MS 3996AU, 45, SC818 45, SC818 45, SDM 450, SDM 710, SDM 710, SDM 710, SDM 710, SDM	APQ800 Q8053, APQ809 DM9607 DM9605 DM9655 MB909, MSM8916, MSM8937, SM8940, SM8937, SM8940, SM8937, SM8940, SM8937, SM8955 SM8955, MSM89 Elfon, SD Elfon, SD Elfon, SD Elfon, SD Elfon, SD Elfon, SD Elfon, SD Elfon, SD Elfon, SM Elfon, SM	9, 8, 5, 40, 5, 40, 5, 40, 7, 5, 40, 60, M439, M632, M670, M850, , 8150,				
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Mobil Music Wear APQ8 APQ8 MDM	P modulout side it received the sage. Snapdragon Indragon	its bour yes malfo in Snapo agon Cor onsume ndustria oT, Snap lragon V ragon APQ800 Q8053, APQ809	ndary ormed dragon npute, r IOT, dragon oice &	https:/ w.qual m.com pany/j ct- securit lletins, ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- QCM2- 031219	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM896AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID: CVE-2019-2303		
sdx55					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDX5- 031219/1437

3-4

4-5

6-7

7-8

8-9

5-6

9-10

CV Scoring Scale

(CVSS)

0-1

1-2

2-3

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			MSM8 MSM8 MSM8 MSM8 MSM8 QCM2 SC818 SDM6 SDM6 SDM6 SDM8 SDX5 SM81 Snapo	9650, M. 8905, M. 8905, M. 8920, M. 8920, M. 8976, M. 8976, M. 8150, Q. 80X, SDM 845, SDM 845, SDM 845, SDM 845, SM61! 8130, SX D: CVE-	5M8909, MSM8937, 5M8953, 5M8996, cobar, S605, Q 1632, SD 1632, SD 1632, SD 1670, SD 1850, SM7 250, High_Me R2130	M215, AU, M215, A845, M450, M636, M710, X20, 150,				
Use After Free	21-11-2019	4.9	listen memo use af Snapo	equent user may repry corructer free dragon Adragon Chagon Indragon Waragon Verructure orking in 104, SDX5 50, SM8	result in uption d issue, in uto, compute connective doustriand of the work of	further ue to vity, or IOT, I IOT, Music, 205, 150, R2130	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ cy/bu /octo 19-	H-QUA- 031219	
Improper Restriction of Operations within the	21-11-2019	7.2	lack o array image	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in pany/p Snapdragon Auto, https://www.qualcommons.com/pany/p			com /com	H-QUA- 031219		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
Bounds of a Memory Buffer			Snapo Snapo Snapo Snapo Infras Netwo QCS40 SDM6 SDM8 SM61 SXR1	lragon C lragon C lragon Ir lragon M lragon W tructure orking in 04, QCS6 70, SDM 50, SM7 50, SM7 130, SXR	onnective onsume ndustria Jobile, Vired and MDM9 05, SDA 710, SD 24, SDX 150, SM	vity, r IOT, l IOT, 205, 845, M845, 55, 8150,	securit lletins ber-20 bulleti	/octo 119-		
Out-of- bounds Read	21-11-2019	10	while session messar un-information of Snapor Snapor Snapor Snapor Snapor Snapor Snapor Snapor Snapor Mobil Music Wears APQ8 APQ8 MDM MDM MDM MDM MDM MDM MSM8 MSM8 MSM8	r over reparsing namages if netended valuagen Caragon Caragon Interpretation (Caragon Interpretation) (Caragon Interpreta	downlingement (etwork stalues in uto, ompute, onsume ndustria oT, Snap ragon APQ800 Q8053, APQ809 DM9607 DM9605 DM	nk OTA ends  r IOT, l IOT, dragon oice &  9,  8,  7,  40,  7,  77,	https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-: 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDA8 SDM4 SDM6 SDM7 SDX2 SM61 SM82 Snapo , SXR1	.5, SC81; 45, SDM .50, SDM .36, SDM .10, SDX24 .50, SM7 .50, .dragon_H .130, SX .D: CVE-	429, SD 1630, SD 1660, SD 1845, SD 1, SDX55 150, SM High_Me R2130	M439, M632, M670, M850, 5, 8150, d_2016				
Improper Authenticati on	21-11-2019	10	Lack of allow NAS in result bypas Snapo Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM8 MS	of integral of integral of integral of into autors of NAS dragon of integration o	ity check M to access which a chentical in auto, compute consume adustrial oT, Snap largon APQ800 Q8053, APQ809 DM9605 DM9625 DM9625 DM9625 DM9625 MSM8937, SM8940, SM8937, SM8940, MSM8937, SM8940, MSM8	k ept any can tion  or IOT, odragon voice & ept any can tion  8, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10	https:/w.qualm.company/jct-securitiletinsber-20bulleti	com /com produ ty/bu /octo	H-QUA-: 031219	
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	C ID
			SDM7 SDX2 SM61 SM82 Snapo , SXR1	lragon_I L130, SX <b>D : CVE-</b>	1845, SD 4, SDX55 150, SM High_Me R2130 <b>2019-2</b>					
Out-of- bounds Read	21-11-2019	7.5	array when XID m Auto, Snapo Snapo Snapo Mobil Music Wears APQ8 MDM MDM MDM MDM MDM MSM8 MSM8 MSM8 MSM	P modulout side it receive essage. Snapdradragon Idragon Idrag	its bounces malfed in Snaped agon Cordonsume industria oT, Snaped agon Veragon	ndary ormed dragon inpute, ar IOT, I IOT, idragon foice & 9, 8, 5, 7, 6, 40, 5, 7, 6, 40, 6, 6, 4660, M439, M632, M670, M850, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6,	https:/ w.qual m.com pany/i ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA-9 031219	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	n & CVE	ID	Pat	ch	NCIIP	C ID
			_	dragon_F 1130, SX	_	d_2016				
			CVE I	D : CVE-	2019-2	303				
Use After Free	21-11-2019	7.2	cleand missing for a fapplic Comp Consu Indus Mobil Infras Netwood QCS40 SDX50 SDX50 SM81	fter free up routing points failed station. in oute, Snaparial IOT e, Snaparial IOT e, Snaparial IOT, QCS6 570, SDM 5, SM615 50, SXR1	ne due to er saniti rt of a to Snapdr pdragor C, Snapdo ragon V e and MDM9 05, SDA 710, SD 50, SM7	zation rusted ragon ragon ragon Vired 205, 845, M845, 150,	https:/ w.qual m.com pany/j ct- securii lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	
apq8064										
Integer Underflow (Wrap or Wraparound )	21-11-2019	4.6	while stand user's Auto, Electric Snape Snape Snape Infras Network APQ8 APQ8 IPQ40 MDM MDM MDM	Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8052		https:/ w.qual m.com pany/j ct- securit lletins ber-20 bulleti	com /com produ ty/bu /octo	H-QUA- 031219	•	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID: CVE-2019-2297		
apq8096					
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8953, MSM8996, MSM896AU, APQ8098, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, MSM8953, MSM8996, SDM630, SDM632, SDM636, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8- 031219/1445

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130		
			CVE ID : CVE-2019-2315		
Out-of- bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8940, MSM8953, MSM8996, MSM896AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID: CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8- 031219/1446
Schneider-ele	ectric				
bmx_p34x					
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which	https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019- 281-02/	H-SCH-BMX 031219/1447
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	escription	on & CVE	ID	Pat	tch	NCIIF	PC ID
			FTP ha when u of the o unsecu	ardcode using th controll are netw	d crede ie Web s ler on ai	server 1				
bmx_noe_010	0									
Information Exposure	20-11-2019	5	Exposi in Mod (M340 commit Premit commit Quantit commit see sec specifi could of FTP ha when to of the of unsecu	are vuln licon Co CPUs, l unication um CPU unication um CPU unication curity n c version cause the ardcode using the controll	ontroller M340 on modu is, Prem on modu otificati ons), wh he disclored de crede he Web s	cy exists cs ales, ium ales, tum ales - on for ich osure of ntials server	https:/ w.schr - electri /ww/o wnloa ument D-201 281-0	c.com en/do d/doc c/SEV	H-SCH- 031219	_
bmx_noe_011	0									
Information Exposure	20-11-2019	5	Exposi in Mod (M340 commit commit Quanti commit see sec specifi could of FTP ha	are vuln licon Co CPUs, l unication um CPU unication curity n c version cause the	ontrolle	y exists  cs  ales, ium ales, tum ales - on for ich osure of ntials	https:/ w.schr - electri /ww/e wnloa ument D-201 281-02	c.com en/do d/doc c/SEV 9-	H-SCH- 031219	_
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	ch	NCIIP	CID
				control ure netv	ler on an	1				
					vork. 2 <b>019-6</b>	052				
hwy nog 040	1		CVEI	D: CVE-	2019-0	854				
bmx_noc_040	1		A CIAI	E 200. I	nformati					
Information Exposure	20-11-2019	5	Exposin Mo (M34 comm Prem comm Quant see se second FTP h when of the unsec	Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.  CVE ID: CVE-2019-6852				//ww neider c.com en/do d/doc c/SEV 9-	H-SCH-F 031219	_
tsx_p57x										
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.  CVE ID: CVE-2019-6852				https:/ w.schr - electri /ww/e wnloa ument D-201 281-02	c.com en/do d/doc e/SEV	H-SCH-7 031219	
			CVE I	D : CVE-	2019-6	852				

Weakness	Publish Date	CVSS	1	Description	on & CVE	ID	Pat	ch	NCIIP	C ID
tsx_ety_x103										
Information Exposure	20-11-2019	5	Exposin Mo (M34 comm Premiscomm Quant comm see see see see see see see see see s	E-200: In sure vuln dicon Co O CPUs, I nunication CPU nunication CPU nunication curity no fic version cause the ardcode using the controll cure network of the controll of the control of the co	nerability ontroller M340 on modu s, Premi on modu otifications), whe he disclouded credes he Web s ler on an	y exists  cs  cles, ium cles, tum cles - on for ich esure of ntials server	https:/ w.schr - electri /ww/e wnloa ument D-201 281-02	c.com en/do d/doc e/SEV	H-SCH-7 031219	
140_cpu6x			U.Z.	<b>D</b> . G. E						
Information Exposure	20-11-2019	5	Exposin Mo (M34 comm Premiscomm Quant comm see see see see see see see see see s	E-200: In sure vuln dicon Co of CPUs, In unication the country in cause the cause the control of the control of the countrol o	nerability ontroller M340 on modu (s, Premis on modu otifications), whe he disclosed credes he Web s ler on an	y exists  Iles, ium Iles, tum Iles - on for ich isure of ntials server	https:/ w.schr - electri /ww/e wnloa ument D-201 281-02	c.com en/do d/doc e/SEV	H-SCH-1 031219	_
140_noe_771	x1									
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists				https:/ w.schr	-	H-SCH-1 031219	
CV Scoring Scal (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	ch	NCIIP	CID			
			in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.  CVE ID: CVE-2019-6852				electri /ww/e wnload ument D-201 281-02	en/do d/doc /SEV 9-					
140_noc_78x0	00												
Information Exposure	20-11-2019	5	Exposin Mo (M34 comm Prem comm Quant see se specific could FTP h when of the	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of				//ww neider c.com en/do d/doc /SEV 9- 2/	H-SCH-1 031219	_			
140_noc_7710	01												
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules,				Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340			https://w.schr - electri /ww/e	eider c.com	H-SCH-1 031219	_
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6			6-7	7-8	8-9	9-10				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.  CVE ID: CVE-2019-6852	wnload/doc ument/SEV D-2019- 281-02/		
ztehome						
c520v21						
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-11-2019	5	permission and access control vulnerability, which exists in V2.1.14 and below versions of C520V21 smart camera devices. An attacker can construct a URL for directory traversal and access to other unauthorized files or resources.  CVE ID: CVE-2019-3423	http://supp ort.zte.com. cn/support /news/Loo pholeInfoD etail.aspx?n ewsId=101 1842	H-ZTE-C520- 031219/1457	
Improper Authenticati on	18-11-2019	6.4	authentication issues vulnerability, which exists in V2.1.14 and below versions of C520V21 smart camera devices. An attacker can automatically obtain access to web services from the authorized browser of the same computer and perform operations.  CVE ID: CVE-2019-3424	http://supp ort.zte.com. cn/support /news/Loo pholeInfoD etail.aspx?n ewsId=101 1842	H-ZTE-C520- 031219/1458	

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