National Critical Information Infrastructure Protection CentreCommon Vulnerabilities and Exposures(CVE) Report									
Topic of MIND			16 - 31 Jul 2019	Vol. (6 No. 14				
Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			Application						
Adobe									
dreamweav	ver								
Untrusted Search Path	18-07-2019	6.8	Adobe Dreamweaver direct download installer versions 19.0 and below, 18.0 and below have an Insecure Library Loading (DLL hijacking) vulnerability. Successful exploitation could lead to Privilege Escalation in the context of the current user.	N/A	A-ADO-DREA- 130819/1				
			CVE ID : CVE-2019-7956						
bridge_cc									
Out-of- bounds Read	18-07-2019	4.3	Adobe Bridge CC version 9.0.2 and earlier versions have an out of bound read vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user. CVE ID : CVE-2019-7963	N/A	A-ADO-BRID- 130819/2				
campaign									
Improper Input Validation	18-07-2019	5	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Insufficient input validation vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user. CVE ID : CVE-2019-7843	N/A	A-ADO-CAMP- 130819/3				
N/A	18-07-2019	5	Adobe Campaign Classic	N/A	A-ADO-CAMP-				
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	C	escriptic	on & CVE	Pa	tch	NCII	NCIIPC ID	
			earlier Improp vulnera exploita Inform context	18.10.5 versions ability. S ation co ation Di	s have a r handlin uccessfu uld lead sclosure current u	n ng 1l to e in the 1ser.			130819	9/4
			CVE ID	: CVE-2	019-78	46				
Improper Restriction of XML External Entity Reference ('XXE')	18-07-2019	5	Adobe version earlier Improp Externa ('XXE') Success lead to to the f context CVE ID	ind n of XML nce could access e iser.	N/A		A-ADO- 130819			
Improper Access Control	18-07-2019	5	Adobe version earlier Inadequ vulnera exploita Informa context	and n crol al to e in the aser.	N/A		A-ADO- 130819			
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	18-07-2019	7.5	version earlier Comma vulnera exploita Arbitra the con	uccessfi uld lead Executi	und 11 to on in ent user.	N/A		A-ADO-CAMP- 130819/7		
Informatio	18-07-2019	5	Adobe	gn Class	ic	N/A		A-ADO-	CAMP-	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publi	sh Date	CVSS	I	Descriptio	on & CVE	Pa	tch	NCIIP	PC ID	
n Exposure				earlier Inform Throug vulner exploit Inform	n 18.10.5 version ation Ex gh an Ern ability. S ation co ation Di t of the c	s have a posure cor Mess uccessfi uld lead sclosure	n sage 1l to e in the			130819	/8
				CVE ID) : CVE-2	019-79	41				
experience_	mana	ger		-						Γ	
Cross-Site Request Forgery (CSRF)	18-07	7-2019	4.3	version Cross-S vulner exploit Sensiti disclos curren		l ealier h uest For uccessfu uld lead mation ne conte	nave a gery 1l to xt of the	N/A		A-ADO- 130819	
Impropor											
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-07	7-2019	4.3	version Stored vulner exploit Sensiti disclos curren	Adobe Experience Manager version 6.4 and ealier have a Stored Cross-site Scripting vulnerability. Successful exploitation could lead to Sensitive Information disclosure in the context of the current user. CVE ID : CVE-2019-7954					A-ADO- 130819	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-07	7-2019	5.8	version Reflect vulner exploit Sensiti disclos curren		l ealier h s-site Sc uccessfu uld lead mation ne conte	nave a ripting ıl to xt of the	N/A		A-ADO- 130819	
ajdg											
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	l	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
adrotate	I										
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	23-07-	2019	6.5	before allows	dG AdRc 5.3 for V SQL Inje) : CVE-2	VordPre ection.	ess	g.solu /2019 11/ac e-pro impor	9/07/ drotat -5-3- rtant- ce-for- ity-	A-AJD-A 130819	
akeo											
rufus				Alza	oncultin	a Dufue	20 and				
Uncontroll ed Search Path Element	19-07-	2019	6.8	earlier search impact execut privile Execut execut on the vector 426, CV	is affect order hi is: Arbit ion WIT ge. The c able inst ables (A web site is: CAPE WE-427.	ed by: D ijacking. trary coo H escala compone callers, p LL execu). The a C-471, (LL The de tion of ent is: oortable itables ttack CWE-	N/A		A-AKE- 130819	
N/A	19-07-	2019	7.5	earlier Permis arbitra escalat compo installe (ALL e: The att CWE-3	onsultin is affect sions. T ion of pr nent is: er, porta xecutabl tack vect 77, CWE 0: CVE-2	ed by: In he impa executio rivilege. Executa ble exec es availa for is: CV 5-379.	nsecure ct is: on with The ble utable able). WE-29,	N/A		A-AKE- 130819	
Altn											
mdaemon_e	email_s	erver									
CV Scoring So (CVSS)	cale	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	Pa	tch	NCIIF	'C ID	
Improper Input Validation	16-07-2019	5	skips S default larger checks special arguab curren sizes. T risk ma e-mail, server resour messag	non Ema pamAssa for e-ma than 2 M to 10 M configue ly incom thy popu this migh anageme if a cust with suf ces to sc ges.	assin ch ail mess (B (and) B even v ration), sistent v lar mess nt interf ent for m omer de ficient an large	ecks by ages limits with which is vith sage ere with halicious eploys a	N/A		A-ALT-1 130819	
antsword_p	oroject								•	
antsword										
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	19-07-2019	4.3	XSS in configu executi module s, module dex.js, module module js.	modules/database/custom/in dex.js, modules/database/index.js, or modules/database/php/index.					A-ANT- 130819	
Avast										
antivirus			In A	λ	mah-f	no 10 4				
Improper Link Resolution Before File Access ('Link Following')	18-07-2019	3.6	a local the pro arbitra Logs\U symlin produc	trator ca o renam	cing the ith a the rite to	N/A		A-AVA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			symlink is renamed. This defect can be exploited to rename a critical product file (e.g., AvastSvc.exe), causing the product to fail to start on the next system restart.		
			CVE ID : CVE-2019-11230		
axiosys					
bento4					
NULL Pointer Dereferenc e	18-07-2019	4.3	In Bento4 1.5.1-627, AP4_DataBuffer::SetDataSize does not handle reallocation failures, leading to a memory copy into a NULL pointer. This is different from CVE-2018- 20186. CVE ID : CVE-2019-13959	N/A	A-AXI-BENT- 130819/18
b3log					
wide					
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	18-07-2019	5	b3log Wide before 1.6.0 allows three types of attacks to access arbitrary files. First, the attacker can write code in the editor, and compile and run it approximately three times to read an arbitrary file. Second, the attacker can create a symlink, and then place the symlink into a ZIP archive. An unzip operation leads to read access, and write access (depending on file permissions), to the symlink target. Third, the attacker can import a Git repository that contains a symlink, similarly leading to read and write access.	N/A	A-B3L-WIDE- 130819/19

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-13915		
bacnet_prot	tocol_stack_pr	oject			
bacnet_prot	tocol_stack				
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-07-2019	6.8	BACnet Stack bacserv 0.9.1 and 0.8.5 is affected by: Buffer Overflow. The impact is: exploit was not explored. The component is: bacserv BVLC forwarded NPDU. bvlc_bdt_forward_npdu() calls bvlc_encode_forwarded_npdu() which copies the content from the request into a local in the bvlc_bdt_forward_npdu() stack frame and clobbers the canary. The attack vector is: A BACnet/IP device with BBMD enabled based on this library connected to IP network. The fixed version is: 0.8.6. CVE ID : CVE-2019-1010073	N/A	A-BAC-BACN- 130819/20
cat_runner_	_ _decorate_hom	e_proj	ect		
	_decorate_hom				
Improper Input Validation	22-07-2019	5	The application API of Cat Runner Decorate Home version 2.8.0 for Android does not sufficiently verify inputs that are assumed to be immutable but are actually externally controllable. Attackers can manipulate users' score parameters exchanged between client and server. CVE ID : CVE-2019-13097	N/A	A-CAT-CAT 130819/21
centos-web	panel			l	
centos_web	_panel				

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	[Descriptio	on & CVE	ID	Pa	tch	NCIIF	PC ID
Unrestricte d Upload of File with Dangerous Type	16-07-2019	8.5	CWP) (0.9.8.8 allows and up /tmp d become	CentOS V 36, a cw a norma load a so irectory e the roo	Veb Pan psrv-xx: al user to ession fi r, and us	x cookie o craft le to the e it to	N/A		A-CEN- 130819	
Improper Authentica tion	16-07-2019	7.5	CWP) (0.9.8.83 can byp the log knowle userna	CentOS V 36, remo bass aut in proce edge of a me.	Veb Pan ote attac henticat ss by lev	kers tion in veraging	N/A		A-CEN- 130819	
Informatio n Exposure	16-07-2019	5	CWP) (0.9.8.84 allows whethe by read	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.846, the Login process allows attackers to check whether a username is valid by reading the HTTP response. CVE ID : CVE-2019-13383					A-CEN- 130819	
Improper Authentica tion	16-07-2019	6.5	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.838 to 0.9.8.846, remote attackers can bypass authentication in the login process by leveraging the knowledge of a valid username. The attacker must defeat an encoding that is not equivalent to base64, and thus this is different from CVE- 2019-13360. CVE ID : CVE-2019-13605				N/A		A-CEN- 130819	
central_dog										
central_dog	ma									
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	26-07-2019	4.3	Cross-site scripting vulnerability in Central Dogma 0.17.0 to 0.40.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. CVE ID : CVE-2019-6002	N/A	A-CEN-CENT- 130819/26
Cherokee-p	roject				-
cherokee_w	vebserver				
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	5	Cherokee Webserver Latest Cherokee Web server Upto Version 1.2.103 (Current stable) is affected by: Buffer Overflow - CWE-120. The impact is: Crash. The component is: Main cherokee command. The attack vector is: Overwrite argv[0] to an insane length with execl. The fixed version is: There's no fix yet. CVE ID : CVE-2019-1010218	N/A	A-CHE-CHER- 130819/27
Cisco	<u> </u>			<u> </u>	
vision_dyna	mic_signage_c	lirecto	r		
Improper Authentica tion	17-07-2019	10	A vulnerability in the REST API interface of Cisco Vision Dynamic Signage Director could allow an unauthenticated, remote attacker to bypass authentication on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could	N/A	A-CIS-VISI- 130819/28
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary actions through the REST API with administrative privileges on the affected system. The REST API is enabled by default and cannot be disabled. CVE ID : CVE-2019-1917		
findit_netw	ork_manager				
Use of Hard- coded Credential s	17-07-2019	7.2	A vulnerability in the Cisco FindIT Network Management Software virtual machine (VM) images could allow an unauthenticated, local attacker who has access to the VM console to log in to the device with a static account that has root privileges. The vulnerability is due to the presence of an account with static credentials in the underlying Linux operating system. An attacker could exploit this vulnerability by logging in to the command line of the affected VM with the static account. A successful exploit could allow the attacker to log in with root- level privileges. This vulnerability affects only Cisco FindIT Network Manager and Cisco FindIT Network Probe Release 1.1.4 if these products are using Cisco-supplied VM images. No other releases or deployment models are known to be vulnerable. CVE ID : CVE-2019-1919	N/A	A-CIS-FIND- 130819/29

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

Γ

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	CID
industrial_r	network_direc	tor								
N/A	17-07-2019	4.3	Service (WSMA Industri (IND) of unauth attacket read ac using a certific due to certific establi connect establi connect supply certific connect success the atta in-the- decryp inform connect softwa publica affecte release	erability es Manag A) featur rial Netv could all enticate er to gain ccess to s in invalio rate. The insuffici rate valic shing a V ction. An cthis vul ing a cra cate duri ction setu sful expl acker to middle a t confide ation on ctions to re. At the ation, thi d Cisco I es prior to D : CVE-2	gement A e of Cisc vork Dir ow an ed, remo n unauth sensitive d X.509 vulnera ent X.50 lation w WSMA attacke nerabili fted X.5 ng the V up phas oit coul- conduct attacks t ential WSMA the affe e time o s vulner ND Soft co 1.7.	Agent co rector te norized e data ability is 09 when r could ty by 09 VSMA e. A d allow t man- o cted f cability ware	N/A		A-CIS-II 130819	
identity_ser	vices_engine								1	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	based i of Cisco Engine unauth attacke site scr against	erability manager o Identit e (ISE) co enticate er to con ripting (2 t a user o manager	nent int y Servic ould allo d, remo duct a c KSS) atta of the we	erface es w an te ross- ack eb-	N/A		A-CIS-II 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	C ID
			success the atta arbitra contex interfa browse the tim vulnera runnin prior te	ause ement oerly input. oit this ading a s link. A d allow the sitive, ation. At , this Cisco ISE ses nd 2.6.0.						
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-07-2019	4	CVE ID : CVE-2019-1941 A vulnerability in the sponsor portal web interface for Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. At the time of publication, this vulnerability affected Cisco ISE running software releases				N/A		A-CIS-II 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.6.0 and prior.		
			CVE ID : CVE-2019-1942		
findit_netw	ork_probe				
Use of Hard- coded Credential s	17-07-2019	7.2	A vulnerability in the Cisco FindIT Network Management Software virtual machine (VM) images could allow an unauthenticated, local attacker who has access to the VM console to log in to the device with a static account that has root privileges. The vulnerability is due to the presence of an account with static credentials in the underlying Linux operating system. An attacker could exploit this vulnerability by logging in to the command line of the affected VM with the static account. A successful exploit could allow the attacker to log in with root- level privileges. This vulnerability affects only Cisco FindIT Network Manager and Cisco FindIT Network Probe Release 1.1.4 if these products are using Cisco-supplied VM images. No other releases or deployment models are known to be vulnerable. CVE ID : CVE-2019-1919	N/A	A-CIS-FIND- 130819/33
cjson_proje cjson	ct				
Improper			DaveGamble/cJSON cJSON		
Check for Unusual or Exceptiona	19-07-2019	5	1.7.8 is affected by: Improper Check for Unusual or Exceptional Conditions. The	N/A	A-CJS-CJSO- 130819/34
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9 -10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Pat	tch	NCIIP	PC ID
l Conditions			impact attack of service cJSON_ itive() f vector fixed ve CVE ID							
Cmsmadesi	mple									
Bable:multi	lingual_site									
URL Redirectio n to Untrusted Site ('Open Redirect')	5.8	All is af Redirect Redirect is supp "newur compor The att victim r created Attacket legitim redirect his/her	Multiling fected b ction. Th ction to a lied to r l' param nent is: n ack vect must op l by an a er may u ate site n t user to choosin : CVE-2	y: Open ne impac any URL edirect.j neter. Th redirect for is: Th en a link ttacker. se any using Ba o a URL o ng.	et is: , which ohp in a he .php. he c	N/A		A-CMS- 130819		
code42									I	
code42										
Improper Access Control	19-07-2019	6.5	In Code42 for Enterprise through 6.8.4, an administrator without web restore permission but with the ability to manage users in an organization can impersonate a user with web restore permission. When requesting the token to do a web restore, an administrator with permission to manage a user could request the token of				port.c 2.com ms_ar nditio ode42 omer_ ort_re es/Co _secu	A/Ter ad_co ons/C 2_cust _supp esourc de42 rity_a rity_a	A-COD- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that user. If the administrator was not authorized to perform web restores but the user was authorized to perform web restores, this would allow the administrator to impersonate the user with greater permissions. In order to exploit this vulnerability, the user would have to be an administrator with access to manage an organization with a user with greater permissions than themselves. CVE ID : CVE-2019-11553	calation_in_ LoginToke n_API	
Comodo			CVE ID : CVE-2019-11555		
antivirus					
N/A	17-07-2019	7.2	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to Local Privilege Escalation due to CmdAgent's handling of COM clients. A local process can bypass the signature check enforced by CmdAgent via process hollowing which can then allow the process to invoke sensitive COM methods in CmdAgent such as writing to the registry with SYSTEM privileges. CVE ID : CVE-2019-3969	N/A	A-COM-ANTI- 130819/37
Improper Input Validation	17-07-2019	2.1	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to Arbitrary File Write due to Cavwp.exe handling of Comodo's Antivirus database. Cavwp.exe loads Comodo antivirus definition database in unsecured global section	N/A	A-COM-ANTI- 130819/38
CV Scoring So			22 24 45 56		

(0033)						<u> </u>		<u> </u>		
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
			objects, allowing a local low privileged process to modify this data directly and change virus signatures.		
			CVE ID : CVE-2019-3970		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-07-2019	2.1	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to a local Denial of Service affecting CmdVirth.exe via its LPC port "cmdvrtLPCServerPort". A low privileged local process can connect to this port and send an LPC_DATAGRAM, which triggers an Access Violation due to hardcoded NULLs used for Source parameter in a memcpy operation that is called for this handler. This results in CmdVirth.exe and its child svchost.exe instances to terminate. CVE ID : CVE-2019-3971	N/A	A-COM-ANTI- 130819/39
Out-of- bounds Read	17-07-2019	2.1	Comodo Antivirus versions 12.0.0.6810 and below are vulnerable to Denial of Service affecting CmdAgent.exe via an unprotected section object " <guid>_CisSharedMemBuff". This section object is exposed by CmdAgent and contains a SharedMemoryDictionary object, which allows a low privileged process to modify the object data causing CmdAgent.exe to crash. CVE ID : CVE-2019-3972</guid>	N/A	A-COM-ANTI- 130819/40
Out-of- bounds	17-07-2019	4.9	Comodo Antivirus versions 11.0.0.6582 and below are	N/A	A-COM-ANTI- 130819/41
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			vulnerable to Denial of Service affecting CmdGuard.sys via its filter port "cmdServicePort". A low privileged process can crash CmdVirth.exe to decrease the port's connection count followed by process hollowing a CmdVirth.exe instance with malicious code to obtain a handle to "cmdServicePort". Once this occurs, a specially crafted message can be sent to "cmdServicePort" using "FilterSendMessage" API. This can trigger an out-of-bounds write if lpOutBuffer parameter in FilterSendMessage API is near the end of specified buffer bounds. The crash occurs when the driver performs a memset operation which uses a size beyond the size of buffer specified, causing kernel crash.		
			CVE ID : CVE-2019-3973		
computerla	b				
maple_com	puter_wbt_snn	np_adn	ninistrator		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-07-2019	7.5	SnmpAdm.exe in MAPLE WBT SNMP Administrator v2.0.195.15 has an Unauthenticated Remote Buffer Overflow via a long string to the CE Remote feature listening on Port 987. CVE ID : CVE-2019-13577	N/A	A-COM- MAPL- 130819/42
Cpanel					
cpanel					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				17						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	30-07-2019	3.5	cPanel before 82.0.2 has stored XSS in the WHM Tomcat Manager interface (SEC-504). CVE ID : CVE-2019-14386	N/A	A-CPA-CPAN- 130819/43
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	30-07-2019	4.3	cPanel before 82.0.2 has Self XSS in the cPanel and webmail master templates (SEC-506). CVE ID : CVE-2019-14387	N/A	A-CPA-CPAN- 130819/44
Improper Input Validation	30-07-2019	5	cPanel before 82.0.2 allows unauthenticated file creation because Exim log parsing is mishandled (SEC-507). CVE ID : CVE-2019-14388	N/A	A-CPA-CPAN- 130819/45
N/A	30-07-2019	2.1	cPanel before 82.0.2 allows local users to discover the MySQL root password (SEC- 510). CVE ID : CVE-2019-14389	N/A	A-CPA-CPAN- 130819/46
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	30-07-2019	3.5	cPanel before 82.0.2 has stored XSS in the WHM Modify Account interface (SEC-512). CVE ID : CVE-2019-14390	N/A	A-CPA-CPAN- 130819/47
N/A	30-07-2019	2.1	cPanel before 82.0.2 does not properly enforce Reseller	N/A	A-CPA-CPAN- 130819/48
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 18	6-7 7-8	8-9 9-10

Weakness	Publish	n Date	CVSS	Description & CVE ID					tch	NCIIP	PC ID
				packag 514).	e creatio	on ACLs	(SEC-				
				CVE ID	: CVE-2	019-14	391				
Improper Input Validation	30-07-	2019	6.5	remote demo a incorre (SEC-5	-	ecution because lispatch	by a of ing	umen .cpano /disp L/80-	lay/C ⊦Chan	A-CPA-0 130819	
) : CVE-2	019-14	392	ge+Lo	og		
Dancer::plu				ject							
Dancer::plu	gin::sin	nplecru	ıd								
Improper Access Control	17-07-	2019	4	1.14 ar Incorre impact unatho The co calls to wrapp authen being a	::Simple r is affects ss Contr ntial for cess to o t is: Inco e_auth() : in -checkir o al rou 2019-10	cted by: ol. The lata. orrect ng not tes.	N/A		A-DAN- 130819	_	
Dell				<u> </u>							
emc_unity_	operatir	ng_envi	ironme	ent							
Improper Authorizati on	18-07-	2019	4	EntDell EMC Unity and UnityVSAversions prior to 5.0.0.0.5.116contain an improperauthorization vulnerability inNAS Server quotasconfiguration. A remoteauthenticated UnisphereOperator could potentiallyexploit this vulnerability toedit quota configuration ofother users.CVE ID : CVE-2019-3734				N/A		A-DEL- 130819	
Protection	18-07-	2019	2.1	Dell EN	AC Unity	and Un	ityVSA	N/A		A-DEL-	EMC
CV Scoring So (CVSS)	cale	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	Ра	tch	NCIIF	PC ID
Mechanis m Failure			contain a plain-text password storage vulnerability. A Unisphere user?s (including the admin privilege user) password is stored in a plain text in Unity Data Collection bundle (logs files for troubleshooting). A local authenticated attacker with access to the Data Collection bundle may use the exposed password to gain access with the privileges of the compromised user.						130819	9/52
ome unitar	sa_operating_e	nviror	CVE ID : CVE-2019-3741							
emc_unityv	Sa_operating_c		r	AC Unity	and IIn	itvVSA				
Improper Authorizati on	18-07-2019	4	Dell EMC Unity and UnityVSA versions prior to 5.0.0.0.5.116 contain an improper authorization vulnerability in NAS Server quotas configuration. A remote authenticated Unisphere Operator could potentially exploit this vulnerability to edit quota configuration of other users. CVE ID : CVE-2019-3734				N/A		A-DEL-1 130819	
Protection Mechanis m Failure	18-07-2019	2.1	Dell EMC Unity and UnityVSA versions prior to 5.0.0.0.5.116 contain a plain-text password storage vulnerability. A Unisphere user?s (including the admin privilege user) password is stored in a plain text in Unity Data Collection bundle (logs files for troubleshooting). A local authenticated attacker with				N/A		A-DEL-1 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the Data Collection bundle may use the exposed password to gain access with the privileges of the compromised user.		
1.1.			CVE ID : CVE-2019-3741		
deltaww					
cnssoft_scre	eenealtor				
Out-of- bounds Read	24-07-2019	4.3	Delta Electronics CNCSoft ScreenEditor, Versions 1.00.89 and prior. Multiple out-of- bounds read vulnerabilities may cause information disclosure due to lacking user input validation for processing project files. CVE ID : CVE-2019-10992	N/A	A-DEL-CNSS- 130819/55
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-07-2019	6.8	Delta Electronics CNCSoft ScreenEditor, Versions 1.00.89 and prior. Multiple heap-based buffer overflow vulnerabilities may be exploited by processing specially crafted project files, allowing an attacker to remotely execute arbitrary code. There is a lack of user input validation before copying data from project files onto the heap. CVE ID : CVE-2019-10982	N/A	A-DEL-CNSS- 130819/56
dependency	track				
dependency	y-track				
Improper Neutralizat ion of Input During Web Page	29-07-2019	3.5	Dependency-Track before 3.5.1 allows XSS. CVE ID : CVE-2019-1020007	https://git hub.com/D ependency Track/dep endency- track/secu	A-DEP-DEPE- 130819/57
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')				rity/adviso ries/GHSA- jp9v- w6vw- 9m5v	
Dolibarr					
dolibarr				1	
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	Dolibarr 7.0.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: allow malitious html to change user password, disable users and disable password encryptation. The component is: Function User password change, user disable and password encryptation. The attack vector is: admin access malitious urls. CVE ID : CVE-2019-1010054	N/A	A-DOL-DOLI- 130819/58
Domainmo	d				
Domainmo	d				
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can change admin password. The component is: http://127.0.0.1/settings/pass word/ http://127.0.0.1/admin/users /add.php http://127.0.0.1/admin/users /edit.php?uid=2. The attack vector is: After the administrator logged in, open the html page. CVE ID : CVE-2019-1010094	N/A	A-DOM- DOMA- 130819/59
CV Scoring So					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				22						

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIF	PC ID
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	od.org, affecte Forger There : that ca accour http:// /add.p After th in, ope	domainmod(https://domainm od.org/) domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can add the administrator account. The component is: http://127.0.0.1/admin/users /add.php. The attack vector is: After the administrator logged in, open the html page. CVE ID : CVE-2019-1010095					A-DOM DOMA- 130819	
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	od.org affecte Forger There : that ca user to is: http:// /edit.p vector admini the htr	/) doma d by: Cro y (CSRF is a CSRI n chang admin. (127.0.0 hp?uid= is: After istrator nl page.	inmod v oss Site I). The im F vulnera e the rea The com 1/admin 2. The a	ability ability ad-only aponent n/users ttack n, open	N/A		A-DOM DOMA- 130819	
dpic_projec	t									
dpic										
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-07-2019	6.8	dpic 2019.06.20 has a Stack- based Buffer Overflow in the wfloat() function in main.c. CVE ID : CVE-2019-13989				N/A		A-DPI-I 130819	-
eclass			1				1		1	
eclass_ip										
CV Scoring So	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				22						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	25-07-2019	7.5	eClass platform < ip.2.5.10.2.1 allows an attacker to execute SQL command via /admin/academic/studenview _left.php StudentID parameter. CVE ID : CVE-2019-9885	https://zer oday.hitcon .org/vulner ability/ZD- 2019- 00333	A-ECL-ECLA- 130819/63
Eclipse	I			1	I
openj9					
N/A	17-07-2019	4.6	AIX builds of Eclipse OpenJ9 before 0.15.0 contain unused RPATHs which may facilitate code injection and privilege elevation by local users.	https://bu gs.eclipse.o rg/bugs/sh ow_bug.cgi ?id=54805	A-ECL-OPEN- 130819/64
			CVE ID : CVE-2019-11771	5	
Out-of- bounds Write	17-07-2019	7.5	In Eclipse OpenJ9 prior to 0.15, the String.getBytes(int, int, byte[], int) method does not verify that the provided byte array is non-null nor that the provided index is in bounds when compiled by the JIT. This allows arbitrary writes to any 32-bit address or beyond the end of a byte array within Java code run under a SecurityManager. CVE ID : CVE-2019-11772	https://bu gs.eclipse.o rg/bugs/sh ow_bug.cgi ?id=54907 5	A-ECL-OPEN- 130819/65
elcom				J	
elcom_cms					
Improper Neutralizat ion of Special Elements	19-07-2019	5	Elcom CMS before 10.7 has SQL Injection via EventSearchByState.aspx and EventSearchAdv.aspx. CVE ID : CVE-2019-12946	N/A	A-ELC-ELCO- 130819/66
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')					
Espocrm					
espocrm					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	Stored XSS in EspoCRM before 5.6.4 allows remote attackers to execute malicious JavaScript and inject arbitrary source code into the target pages. The attack begins by storing a new stream message containing an XSS payload. The stored payload can then be triggered by clicking a malicious link on the Notifications page.	N/A	A-ESP-ESPO- 130819/67
			CVE ID : CVE-2019-13643		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	28-07-2019	4.3	An issue was discovered in EspoCRM before 5.6.6. There is stored XSS due to lack of filtration of user-supplied data in Create Task. A malicious attacker can modify the parameter name to contain JavaScript code. CVE ID : CVE-2019-14329	N/A	A-ESP-ESPO- 130819/68
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	28-07-2019	4.3	An issue was discovered in EspoCRM before 5.6.6. Stored XSS exists due to lack of filtration of user-supplied data in Create Case. A malicious attacker can modify the firstName and lastName to contain JavaScript code. CVE ID : CVE-2019-14330	N/A	A-ESP-ESPO- 130819/69
Improper	28-07-2019	4.3	An issue was discovered in	N/A	A-ESP-ESPO-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')			EspoCRM before 5.6.6. Stored XSS exists due to lack of filtration of user-supplied data in Create User. A malicious attacker can modify the firstName and lastName to contain JavaScript code. CVE ID : CVE-2019-14331		130819/70
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	28-07-2019	4.3	EspoCRM version 5.6.4 is vulnerable to stored XSS due to lack of filtration of user- supplied data in the api/v1/Document functionality for storing documents in the account tab. An attacker can upload a crafted file that contains JavaScript code in its name. This code will be executed when a user opens a page of any profile with this. CVE ID : CVE-2019-14349	N/A	A-ESP-ESPO- 130819/71
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	28-07-2019	4.3	EspoCRM 5.6.4 is vulnerable to stored XSS due to lack of filtration of user-supplied data in the Knowledge base. A malicious attacker can inject JavaScript code in the body parameter during api/v1/KnowledgeBaseArticle knowledge-base record creation. CVE ID : CVE-2019-14350	N/A	A-ESP-ESPO- 130819/72
N/A	28-07-2019	4	EspoCRM 5.6.4 is vulnerable to user password hash enumeration. A malicious authenticated attacker can brute-force a user password hash by 1 symbol at a time	N/A	A-ESP-ESPO- 130819/73

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				26						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using specially crafted		
			api/v1/User?filterList filters.		
			CVE ID : CVE-2019-14351		
Exim					
exim					
N/A	25-07-2019	10	Exim 4.85 through 4.92 (fixed in 4.92.1) allows remote code execution as root in some unusual configurations that use the \${sort } expansion for items that can be controlled by an attacker (e.g., \$local_part or \$domain). CVE ID : CVE-2019-13917	N/A	A-EXI-EXIM- 130819/74
Exiv2					
exiv2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	28-07-2019	4.3	Exiv2::PngImage::readMetadat a() in pngimage.cpp in Exiv2 0.27.99.0 allows attackers to cause a denial of service (heap-based buffer over-read) via a crafted image file. CVE ID : CVE-2019-14369	N/A	A-EXI-EXIV- 130819/75
Out-of- bounds Read	28-07-2019	4.3	In Exiv2 0.27.99.0, there is an out-of-bounds read in Exiv2::MrwImage::readMetada ta() in mrwimage.cpp. It could result in denial of service. CVE ID : CVE-2019-14370	N/A	A-EXI-EXIV- 130819/76
fanucameri	ca			I	I
robotics_vir	rtual_robot_co	ntrolle	r		
Improper Limitation of a Pathname to a	17-07-2019	5	The remote admin webserver on FANUC Robotics Virtual Robot Controller 8.23 allows Directory Traversal via a forged HTTP request.	N/A	A-FAN-ROBO- 130819/77
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIF	PC ID
Restricted Directory ('Path Traversal')			CVE ID : CVE-2019-13584							
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-07-2019	7.5	The remote admin webserver on FANUC Robotics Virtual Robot Controller 8.23 has a Buffer Overflow via a forged HTTP request. CVE ID : CVE-2019-13585				N/A		A-FAN- 130819	
firefly-iii										
firefly_iii										
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	3.5	Firefly III before 4.7.17.1 is vulnerable to stored XSS due to lack of filtration of user- supplied data in a budget name. The JavaScript code is contained in a transaction, and is executed on the tags/show/\$tag_number\$ tag summary page. CVE ID : CVE-2019-13644				N/A		A-FIR-FIRE- 130819/79	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	3.5	vulner to lack supplie names execut attachi attachi	Firefly III before 4.7.17.3 is vulnerable to stored XSS due to lack of filtration of user- supplied data in image file names. The JavaScript code is executed during attachments/edit/\$file_id\$ attachment editing. CVE ID : CVE-2019-13645			N/A		A-FIR-F 130819	
Improper Neutralizat ion of Input During Web Page	17-07-2019	3.5	Firefly III before 4.7.17.3 is vulnerable to reflected XSS due to lack of filtration of user- supplied data in a search query.			N/A		A-FIR-F 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 28	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Generation ('Cross-site Scripting')			CVE ID : CVE-2019-13646							
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	3.5	Firefly III before 4.7.17.3 is vulnerable to stored XSS due to lack of filtration of user- supplied data in image file content. The JavaScript code is executed during attachments/view/\$file_id\$ attachment viewing. CVE ID : CVE-2019-13647	N/A	A-FIR-FIRE- 130819/82					
Flatcore										
flatcore										
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	A CSRF vulnerability was found in flatCore before 1.5, leading to the upload of arbitrary .php files via acp/core/files.upload- script.php. CVE ID : CVE-2019-13961	N/A	A-FLA-FLAT- 130819/83					
Foliovision										
fv_flowplay	er_video_playo	er								
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-07-2019	10	A SQL injection vulnerability exists in the FolioVision FV Flowplayer Video Player plugin before 7.3.19.727 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system. CVE ID : CVE-2019-13573	https://wo rdpress.org /plugins/fv - wordpress- flowplayer /#develope rs	A-FOL-FV_F- 130819/84					
Foxitsoftwa	re									
phantompdf										
phantompd										
phantompd Uncontroll	21-07-2019	5	An issue was discovered in	N/A	A-FOX-PHAN-					

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIPC ID		
ed Resource Consumpti on			Foxit PhantomPDF before 8.3.11. The application could crash when calling the clone function due to an endless loop resulting from confusing relationships between a child and parent object (caused by an append error).	130819	/85			
			CVE ID : CVE-2019-14207					
NULL Pointer Dereferenc e	21-07-2019	5	getting a PDF object from a document, or parsing a certain portfolio that contains a null dictionary.				PHAN- /86	
Ţ			CVE ID : CVE-2019-14208					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-07-2019	7.5	An issue was discovered in Foxit PhantomPDF before 8.3.10. The application could be exposed to Heap Corruption due to data desynchrony when adding AcroForm. CVE ID : CVE-2019-14209	oxit PhantomPDF before 3.10. The application could e exposed to Heap Corruption he to data desynchrony when dding AcroForm.				
NULL Pointer Dereferenc e	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.10. The application could be exposed to Memory Corruption due to the use of an invalid pointer copy, resulting from a destructed string object. CVE ID : CVE-2019-14210	N/A		A-FOX-PHAN- 130819/88		
Improper Input Validation	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.11. The application could	N/A		A-FOX- 130819		
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIF	PC ID
			crash due to the lack of proper validation of the existence of an object prior to performing operations on that object when executing JavaScript. CVE ID : CVE-2019-14211							
			CVE ID	211						
NULL Pointer Dereferenc e		5	An issue was discovered in Foxit PhantomPDF before 8.3.11. The application could crash when calling certain XFA JavaScript due to the use of, or access to, a NULL pointer without proper validation on the object.		N/A		A-FOX-PHAN- 130819/90			
			CVE ID	: CVE-2	019-14	212				
Improper Input Validation	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.11. The application could crash due to the repeated release of the signature dictionary during CSG_SignatureF and CPDF_Document destruction. CVE ID : CVE-2019-14213				N/A		A-FOX- 130819	
Improper Input Validation	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.10. The application could be exposed to a JavaScript Denial of Service when deleting pages in a document that contains only one page by calling a "t.hidden = true" function. CVE ID : CVE-2019-14214			N/A		A-FOX- 130819		
Improper Input Validation	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.11. The application could crash when calling xfa.event.rest XFA JavaScript			N/A		A-FOX- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 31	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			due to accessing a wild								
			pointer.								
			CVE ID : CVE-2019-14215								
Freedeskto	р										
poppler											
Integer Overflow or Wraparou nd	22-07-2019	4.3	The JPXStream::init function in Poppler 0.78.0 and earlier doesn't check for negative values of stream length, leading to an Integer Overflow, thereby making it possible to allocate a large memory chunk on the heap, with a size controlled by an attacker, as demonstrated by pdftocairo.	https://gitl ab.freedesk top.org/po ppler/popp ler/blob/m aster/NEW S	A-FRE-POPP- 130819/94						
			CVE ID : CVE-2019-9959								
frog_cms_project											
frog_cms	ſ			ſ							
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	22-07-2019	3.5	Frog CMS 1.1 is affected by: Cross Site Scripting (XSS). The impact is: Cookie stealing, Alert pop-up on page, Redirecting to another phishing site, Executing browser exploits. The component is: Snippets. CVE ID : CVE-2019-1010235	N/A	A-FRO-FROG- 130819/95						
gdnsd											
gdnsd											
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-07-2019	7.5	The set_ipv4() function in zscan_rfc1035.rl in gdnsd 3.x before 3.2.1 has a stack-based buffer overflow via a long and malformed IPv4 address in zone data. CVE ID : CVE-2019-13951	N/A	A-GDN-GDNS- 130819/96						
CV Scoring So (CVSS)	CV Scoring Scale (CVSS) 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	Patc	h NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-07-2019	7.5	The set_ipv6() function in zscan_rfc1035.rl in gdnsd before 2.4.3 and 3.x before 3.2.1 has a stack-based buffer overflow via a long and malformed IPv6 address in zone data. CVE ID : CVE-2019-13952	N/A	A-GDN-GDNS- 130819/97
Genetechso	lutions				
pie_register					
Improper Neutralizat ion of Input During 23-07-2019 4.3 Web Page Generation ('Cross-site Scripting')			Genetechsolutions Pie Register 3.0.15 is affected by: Cross Site Scripting (XSS). The impact is: Stealing of session cookies. The component is: File: Login. Parameters: interim-login, wp- lang, and supplied URL. The attack vector is: If a victim clicks a malicious link, the attacker can steal his/her account. The fixed version is: 3.0.16. CVE ID : CVE-2019-1010207	N/A	A-GEN-PIE 130819/98
gitea				1	
gitea					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-07-2019	4.3	Gitea 1.7.0 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Attacker is able to have victim execute arbitrary JS in browser. The component is: go-get URL generation - PR to fix: https://github.com/go- gitea/gitea/pull/5905. The attack vector is: victim must open a specifically crafted URL. The fixed version is: 1.7.1 and later.	N/A	A-GIT-GITE- 130819/99
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID			ID	Pat	tch	NCIIF	PC ID
			CVE ID	: CVE-2	019-10	10261				
glyphandco	g		<u> </u>						<u> </u>	
xpdfreader										
Integer Overflow or Wraparou nd	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an Integer overflow in the function JBIG2Bitmap::combine at JBIG2Stream.cc for the "one byte per line" case. CVE ID : CVE-2019-14288			N/A		A-GLY-2 130819		
Integer Overflow or Wraparou nd	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an integer overflow in the function JBIG2Bitmap::combine at JBIG2Stream.cc for the "multiple bytes per line" case. CVE ID : CVE-2019-14289				N/A		A-GLY-2 130819	
Out-of- bounds Read	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA==6 case 2. CVE ID : CVE-2019-14290			N/A		A-GLY-2 130819		
Out-of- bounds Read	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA==6 case 3. CVE ID : CVE-2019-14291		N/A		A-GLY-XPDF- 130819/103			
Out-of- bounds Read	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA!=6			N/A		A-GLY-2 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			case 1. CVE ID : CVE-2019-14292							
Out-of- bounds Read	27-07-2019	27-07-2019An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA!=6 case 2.		N/A	A-GLY-XPDF- 130819/105					
			CVE ID : CVE-2019-14293							
Use After Free	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is a use- after-free in the function JPXStream::fillReadBuf at JPXStream.cc, due to an out of bounds read.	N/A	A-GLY-XPDF- 130819/106					
			CVE ID : CVE-2019-14294							
GNU	GNU									
patch	1			1						
Improper Link Resolution Before File Access ('Link Following')	17-07-2019	5.8	In GNU patch through 2.7.6, the following of symlinks is mishandled in certain cases other than input files. This affects inp.c and util.c. CVE ID : CVE-2019-13636	N/A	A-GNU-PATC- 130819/107					
binutils										
billutils			GNU binutils gold gold v1.11-							
Improper Input Validation	23-07-2019	4.3	v1.16 (GNU binutils v2.21- v2.31.1) is affected by: Improper Input Validation, Signed/Unsigned Comparison, Out-of-bounds Read. The impact is: Denial of service. The component is: gold/fileread.cc:497, elfcpp/elfcpp_file.h:644. The attack vector is: An ELF file with an invalid e_shoff header	N/A	A-GNU-BINU- 130819/108					
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10					

			field must be opened.							
			neiu must be openeu.							
			CVE ID : CVE-2019-1010204							
Integer Overflow 2 or 2 Wraparou nd	24-07-2019	4.3	An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. simple_object_elf_match in simple-object-elf.c does not check for a zero shstrndx value, leading to an integer overflow and resultant heap- based buffer overflow. CVE ID : CVE-2019-14250	A-GNU-1 130819						
gorul	gorul									
gourl										
Unrestricte d Upload of File with 2 Dangerous Type	23-07-2019	5	GoUrl.io GoURL Wordpress Plugin 1.4.13 and earlier is affected by: CWE-434. The impact is: unauthenticated/unzuthorized Attacker can upload executable file in website. The component is: gourl.php#L5637. The fixed version is: 1.4.14. CVE ID : CVE-2019-1010209	N/A		A-GOR-0 130819				
gpac										
gpac										
Out-of- bounds 1 Read	16-07-2019	5	In GPAC before 0.8.0, isomedia/isom_read.c in libgpac.a has a heap-based buffer over-read, as demonstrated by a crash in gf_m2ts_sync in media_tools/mpegts.c. CVE ID : CVE-2019-13618	N/A		A-GPA-0 130819				
Наргоху										
haproxy										
CV Scoring Scale (CVSS)	le 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 & CVE ID				Pa	tch	NCIIP	C ID
Improper Input Validation	23-07	2-2019	5	attacke service related htx_ma	ers to car (ha_par to		nial of	N/A		A-HAP- 130819	
				CVE ID	: CVE-2	2019-14	241				
helm											
helm											
Improper Certificate Validation	17-07	² -2019	7.5	helm Before 2.7.2 is affected by: CWE-295: Improper Certificate Validation. The impact is: Unauthorized clients could connect to the server because self-signed client certs were aloowed. The component is: helm (many files updated, see https://github.com/helm/hel m/pull/3152/files/1096813bf 9a425e2aa4ac755b6c991b62 6dfab50). The attack vector is: A malicious client could connect to the server over the network. The fixed version is: 2.7.2. CVE ID : CVE-2019-1010275		N/A		A-HEL-1 130819			
hisiphp											
hisiphp											
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	24-07	7-2019	4.3	hisiphp 1.0.8 is affected by: Cross Site Scripting (XSS). CVE ID : CVE-2019-1010193		N/A		A-HIS-H 130819			
CV Scoring So (CVSS)	cale	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	Patch	NCIIPC ID
HP	I				I
arcsight_log	gger				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	24-07-2019	4.3	Mitigates a stored cross site scripting issue in ArcSight Logger versions prior to 6.7.1 CVE ID : CVE-2019-3485	N/A	A-HP-ARCS- 130819/115
icewall_sso	_agent				
Improper Input Validation	19-07-2019	7.1	A security vulnerability in HPE IceWall SSO Agent Option and IceWall MFA (Agent module) could be exploited remotely to cause a denial of service. The versions and platforms of Agent Option modules that are impacted are as follows: 10.0 for Apache 2.2 on RHEL 5 and 6, 10.0 for Apache 2.4 on RHEL 7, 10.0 for Apache 2.4 on RHEL 7, 10.0 for Apache 2.4 on HP- UX 11i v3, 10.0 for IIS on Windows, 11.0 for Apache 2.4 on RHEL 7, MFA Proxy 4.0 (Agent module only) for Apache 2.4 on RHEL 7. CVE ID : CVE-2019-11989	N/A	A-HP-ICEW- 130819/116
mfa_proxy	I				
Improper Input Validation	19-07-2019	7.1	A security vulnerability in HPE IceWall SSO Agent Option and IceWall MFA (Agent module) could be exploited remotely to cause a denial of service. The versions and platforms of Agent Option modules that are impacted are as follows: 10.0 for Apache 2.2 on RHEL 5 and	N/A	A-HP-MFA 130819/117
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			7, 10.0 UX 11i Windov on RHE (Agent Apache	for Apac for Apac v3, 10.0 ws, 11.0 EL 7, MFA module e 2.4 on F e : CVE-2	the 2.4 c for IIS c for Apac A Proxy only) fo RHEL 7.	on HP- on che 2.4 4.0 r				
universal_internet_of_things							-			
Improper Access Control	roper ess 19-07-2019 9		UIoT ve 1.4.1, 1 allow u access a data. H issue in custom 1.6, fixe with 1. custom 1.5, fixe with 1. custom than 1. 1.4.2 an resolut to 1.5 F Custom upgrad version suppor	y vulner ersions 1 .4.0, and inauthor and acce PE has a h HPE UI ers with es are ma 6 RP603 hers with es are ma 5 RP503 hers with 5, such a hd 1.2.4.2 tion will RP503 H hers are p le to the mas or con t for furt 0 : CVE-2	6, 1.5, 1 1.2.4.2 ized ren ss to set ddresse oT: * Fo release ade avai * For release ade avai HF3 * F release s 1.4.0, 2, the be to up F3 or 1.6 requeste updated tact HPl ther assi	1.4.2, could note nsitive d this r UIOT lable UIOT lable or older 1.4.1, grade 5 RP603 ed to L E stance.	N/A		A-HP-U 130819	
ht2labs										
learning_loc	cker									
Improper Neutralizat ion of Input During	16-07-2019	4.3	In HT2 Labs Learning Locker 3.15.1, it's possible to inject malicious HTML and JavaScript code into the DOM of the website via the				N/A		A-HT2- 130819	
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	CID
Web Page Generation ('Cross-site Scripting')			PATH_INFO to the dashboards/ URI. CVE ID : CVE-2019-12834							
IBM							I		1	
spectrum_p	rotect									
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.2	The IBM Spectrum Protect 7.1 and 8.1 Backup-Archive Client is vulnerable to a buffer overflow. This could allow execution of arbitrary code on the local system or the application to crash. IBM X- Force ID: 160200. CVE ID : CVE-2019-4267				N/A		A-IBM-9 130819	
maximo as	set_manageme	ent				07				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-07-2019	5	Manag remote directo attacke special contain (//) to the sys 16288	IBM Maximo Asset Management 7.6 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (//) to view arbitrary files on the system. IBM X-Force ID: 162887. CVE ID : CVE-2019-4430				//ww .com oort/d w.wss ibm1 L73	A-IBM-1 130819	
qradar_secu	urity_informat	tion_an	d_event	_manag	er				1	
Informatio n Exposure	17-07-2019	2.1	IBM QRadar SIEM 7.2 and 7.3 could allow a local user to obtain sensitive information when exporting content that could aid an attacker in further attacks against the system. IBM X-Force ID: 156563. CVE ID : CVE-2019-4054			could allow a local user to obtain sensitive information when exporting content that could aid an attacker in further attacks against the system. IBM X-Force ID: 156563.		//ww a.com oort/d w.wss ibm1 139	A-IBM-0 130819	•
Improper Neutralizat	17-07-2019	3.5	IBM QRadar SIEM 7.2 and 7.3 is vulnerable to cross-site			https: w.ibm	//ww i.com	A-IBM-0	QRAD-	
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159131. CVE ID : CVE-2019-4211	/support/d ocview.wss ?uid=ibm1 0957143	130819/123
Cross-Site Request Forgery (CSRF)	25-07-2019	6.8	IBM QRadar SIEM 7.2 and 7.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 159132. CVE ID : CVE-2019-4212	https://ww w.ibm.com /support/d ocview.wss ?uid=ibm1 0959463	A-IBM-QRAD- 130819/124
cloud_priva	ite				
Informatio n Exposure	25-07-2019 2.1 and 3.1.1 could disclose high sensitive information in installer logs that could be u for further attacks against th system. IBM X-Force ID: 158115.		installer logs that could be use for further attacks against the system. IBM X-Force ID:	N/A	A-IBM-CLOU- 130819/125
N/A	A 25-07-2019 4.6 IBM Cloud 4.6 due to import Force ID:		IBM Cloud Private 3.1.1 and 3.1.2 could allow a local user to obtain elevated privileges due to improper security context constraints. IBM X- Force ID: 162706. CVE ID : CVE-2019-4415	N/A	A-IBM-CLOU- 130819/126
Session Fixation	25-07-2019	4.6	IBM Cloud Private 3.1.0, 3.1.1, and 3.1.2 does not invalidate session after logout which	https://ww w.ibm.com /support/d	A-IBM-CLOU- 130819/127

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

Weakness	Publish Date	CVSS	Description & CVE ID				tch	NCIIP	PC ID
			could allow a impersonate a the system. IB 162949.	another u	ser on	ocviev ?uid= 08848	ibm1		
			CVE ID : CVE-2019-4439						
jazz_for_ser	vice_managen	nent							
Improper Access Control	17-07-2019 4		IBM Jazz for S Management 1.1.3.2 is miss level access co allow a user to authorized re Force ID: 159 CVE ID : CVE -	1.1.3, 1.1. sing funct ontrol tha o delete sources. I 033.	ion at could IBM X-	N/A		A-IBM-J 130819	
icegram									
email_subs	cribers_&_new	sletter	'S						
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	19-07-2019	10	A SQL injection exists in the Io Subscribers & plugin throug WordPress. So exploitation of vulnerability remote attack arbitrary SQL the affected sy CVE ID : CVE -	N/A		A-ICE-E 130819			
I-doit									
i-doit Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL	18-07-2019	7.5	Synetics Gmb earlier is affect Injection. The Unauthenticat database acce component is The attack vec attacker can e vulnerability	N/A		A-I-D-I- 130819	-		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			malicious HTTP POST request. The fixed version is: 1.12.1.		
			CVE ID : CVE-2019-1010248		
Ilias	L			I	
ilias					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	22-07-2019	4.3	Ilias 5.3 before 5.3.12; 5.2 before 5.2.21 is affected by: Cross Site Scripting (XSS) - CWE-79 Type 2: Stored XSS (or Persistent). The impact is: Execute code in the victim's browser. The component is: Assessment / TestQuestionPool. The attack vector is: Cloze Test Text gap (attacker) / Corrections view (victim). The fixed version is: 5.3.12.	N/A	A-ILI-ILIA- 130819/131
jeesite			CVE ID : CVE-2019-1010237		
jeesite					
			Jeesite 1.2.7 is affected by: SQL Injection. The impact is: sensitive information		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	23-07-2019	4	disclosure. The component is: updateProcInsIdByBusinessId() function in src/main/java/com.thinkgem.j eesite/modules/act/ActDao.ja va has SQL Injection vulnerability. The attack vector is: network connectivity,authenticated. The fixed version is: 4.0 and later. CVE ID : CVE-2019-1010201	N/A	A-JEE-JEES- 130819/132

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				40						

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
credentials	binding		I						1	
N/A	19-07-2019	4	Jenkins Credentials Binding Plugin Jenkins 1.17 is affected by: CWE-257: Storing Passwords in a Recoverable Format. The impact is: Authenticated users can recover credentials. The component is: config- variables.jelly line #30 (passwordVariable). The attack vector is: Attacker creates and executes a Jenkins job. CVE ID : CVE-2019-1010241				N/A		A-JEN-CRED- 130819/133	
jenkins										
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-07-2019	4	A path traversal vulnerability in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier in core/src/main/java/hudson/ model/FileParameterValue.jav a allowed attackers with Job/Configure permission to define a file parameter with a file name outside the intended directory, resulting in an arbitrary file write on the Jenkins master when scheduling a build.				N/A		A-JEN-J 130819	
Cross-Site Request Forgery (CSRF)	17-07-2019	5.1	and ear earlier allowin obtain protect CVE ID	okens in rlier, LTS did not ng attack them to tion. • : CVE-2 erability	S 2.176. expire, t ers able bypass 019-10	1 and hereby to CSRF 3 53	N/A N/A		A-JEN-J 130819	/135
Informatio CV Scoring S (CVSS)		1-2	web framework used in 2-3 3-4 4-5 5-6				6-7	7-8	A-JEN-J 8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n Exposure			Jenkins 2.185 and earlier, LTS 2.176.1 and earlier allowed attackers to access view fragments directly, bypassing permission checks and possibly obtain sensitive information.		130819/136
jsish			CVE ID : CVE-2019-10354		
jsish					
NULL Pointer Dereferenc e	23-07-2019	4.3	jsish 2.4.74 2.0474 is affected by: CWE-476: NULL Pointer Dereference. The impact is: denial of service. The component is: function Jsi_StrcmpDict (jsiChar.c:121). The attack vector is: The victim must execute crafted javascript code. The fixed version is: 2.4.77. CVE ID : CVE-2019-1010162	https://jsis h.org/fossil /jsi/tktvie w/5533c4 d665b9683 eebe4d662 493f15eb9 11d1c8f	A-JSI-JSIS- 130819/137
Out-of- bounds Read	23-07-2019	5	Jsish 2.4.77 2.0477 is affected by: Out-of-bounds Read. The impact is: denial of service. The component is: function lexer_getchar (jsiLexer.c:9). The attack vector is: executing crafted javascript code. The fixed version is: 2.4.78. CVE ID : CVE-2019-1010169	N/A	A-JSI-JSIS- 130819/138
Use After Free	23-07-2019	5	Jsish 2.4.77 2.0477 is affected by: Use After Free. The impact is: denial of service. The component is: function Jsi_ObjFree (jsiObj.c:230). The attack vector is: executing crafted javascript code. The fixed version is: 2.4.78.	https://jsis h.org/fossil /jsi/tktvie w/870f496 bb8a70749 1df8026e2f f78b33a5cf 44c1	A-JSI-JSIS- 130819/139

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-101	0170	
NULL Pointer Dereferenc e	23-07-2019	5	Jsish 2.4.83 2.0483 is affe by: Nullpointer dereferen The impact is: denial of service. The component is function jsi_DumpFunctio (jsiEval.c:567). The attact vector is: executing crafte javascript code. The fixed version is: 2.4.84. CVE ID : CVE-2019-101	https://jsis h.org/fossil is: /jsi/tktvie ons w/a3026a k 7c06e0f41 ed af461aa0bc d 2f7a7e886 209390	A-JSI-JSIS- 130819/140
Improper Input Validation	23-07-2019	5	Jsish 2.4.84 2.0484 is affe by: Reachable Assertion. impact is: denial of service The component is: functi Jsi_ValueArrayIndex (jsiValue.c:366). The atta vector is: executing crafte javascript code. The fixed version is: after commit 738ead193aff380a7e3d7 11e446f76867f3. CVE ID : CVE-2019-101	The https://jsis on h.org/fossil /jsi/tktvie ck w/b3278d ed 1a441477d d 50363d28d f79bbf58de 2448af	A-JSI-JSIS- 130819/141
Kaspersky					
anti-virus					
Informatio n Exposure	18-07-2019	4.3	Information Disclosure in Kaspersky Anti-Virus, Kaspersky Internet Secur Kaspersky Total Security versions up to 2019 coul potentially disclose uniqu Product ID by forcing vice visit a specially crafted webpage (for example, vice clicking phishing link). Vulnerability has CVSS v2 base score 2.6 CVE ID : CVE-2019-828	rity, https://sup port.kasper ue sky.com/ge tim to neral/vuln erability.as px?el=1243 0#110719 3.0	A-KAS-ANTI- 130819/142
CV Scoring Se					
(CV Scoring Sc (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		
free_anti-vi	rus						
Informatio n Exposure	18-07-2019	4.3	Information Disclosure in Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security versions up to 2019 could potentially disclose unique Product ID by forcing victim to visit a specially crafted webpage (for example, via clicking phishing link). Vulnerability has CVSS v3.0 base score 2.6 CVE ID : CVE-2019-8286	https://sup port.kasper sky.com/ge neral/vuln erability.as px?el=1243 0#110719	A-KAS-FREE- 130819/143		
internet_security							
Informatio n Exposure	18-07-2019	4.3	Information Disclosure in Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security versions up to 2019 could potentially disclose unique Product ID by forcing victim to visit a specially crafted webpage (for example, via clicking phishing link). Vulnerability has CVSS v3.0 base score 2.6 CVE ID : CVE-2019-8286	https://sup port.kasper sky.com/ge neral/vuln erability.as px?el=1243 0#110719	A-KAS-INTE- 130819/144		
small_office	_security						
Informatio n Exposure	18-07-2019	4.3	Information Disclosure in Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security versions up to 2019 could potentially disclose unique Product ID by forcing victim to visit a specially crafted webpage (for example, via clicking phishing link).	https://sup port.kasper sky.com/ge neral/vuln erability.as px?el=1243 0#110719	A-KAS-SMAL- 130819/145		
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
			Vulnerability has CVSS v3.0		
			base score 2.6		
			CVE ID : CVE-2019-8286		
total_securi	ty			ſ	
Informatio n Exposure	18-07-2019	4.3	Information Disclosure in Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security versions up to 2019 could potentially disclose unique Product ID by forcing victim to visit a specially crafted webpage (for example, via clicking phishing link). Vulnerability has CVSS v3.0 base score 2.6 CVE ID : CVE-2019-8286	https://sup port.kasper sky.com/ge neral/vuln erability.as px?el=1243 0#110719	A-KAS-TOTA- 130819/146
knot-resolv	or				
knot_resolv					
KIIUL_I ESUIV			Alu aughiliteanna diagananad	[
Improper Input Validation	16-07-2019	5	A vulnerability was discovered in DNS resolver component of knot resolver through version 3.2.0 before 4.1.0 which allows remote attackers to bypass DNSSEC validation for non- existence answer. NXDOMAIN answer would get passed through to the client even if its DNSSEC validation failed, instead of sending a SERVFAIL packet. Caching is not affected by this particular bug but see CVE-2019-10191. CVE ID : CVE-2019-10190	https://ww w.knot- resolver.cz /2019-07- 10-knot- resolver- 4.1.0.html	A-KNO-KNOT- 130819/147
Improper Input Validation	16-07-2019	5	A vulnerability was discovered in DNS resolver of knot resolver before version 4.1.0 which allows remote attackers	https://ww w.knot- resolver.cz /2019-07-	A-KNO-KNOT- 130819/148

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				40						

Г

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to downgrade DNSSEC-secur domains to DNSSEC-insecur state, opening possibility of domain hijack using attacks against insecure DNS protoc	e resolver- 4.1.0.html	
			CVE ID : CVE-2019-10191		
ladon_proje	ect				
ladon					
Improper Restriction of XML External Entity Reference ('XXE')	18-07-2019	7.5	Ladon since 0.6.1 (since ebef0aae48af78c159b6fce83 c6f5e7e0ddb059) is affected by: XML External Entity (XXI The impact is: Information Disclosure, reading files and reaching internal network endpoints. The component is SOAP request handlers. For instance: https://bitbucket.org/jakob /ladon/src/42944fc012a3a4 214791c120ee5619434505 7/src/ladon/interfaces/soap y#lines-688. The attack vect is: Send a specially crafted SOAP call.	l E). s: N/A sg 48 06 p.p or	A-LAD-LADO- 130819/149
			CVE ID : CVE-2019-101026	8	
layerbb					
layerbb					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	19-07-2019	4.3	LayerBB 1.1.3 allows XSS via the application/commands/new hp pm_title variable, a relate issue to CVE-2019-17997. CVE ID : CVE-2019-13972	7.p	A-LAY-LAYE- 130819/150
Unrestricte	19-07-2019	7.5	LayerBB 1.1.3 allows	N/A	A-LAY-LAYE-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	CID
d Upload of File with Dangerous Type			file upl custom	/general oad beca _logo fil tricted, a	ause the ename s	-			130819	/151
			CVE ID	: CVE-2	019-13	973				
Cross-Site Request Forgery	19-07-2019	6.8	-	B 1.1.3 a sations.j		d/new	N/A		A-LAY-I 130819	
(CSRF)			CVE ID	: CVE-2	019-13	974				
Libav										
libav									1	
N/A	28-07-2019	4.3	An issue was discovered in Libav 12.3. There is an infinite loop in the function mov_probe in the file libavformat/mov.c, related to offset and tag.						A-LIB-L 130819	
			CVE ID	: CVE-2	019-14	371				
N/A	28-07-2019	4.3	infinite		the fund		N/A		A-LIB-L 130819	
			CVE ID	: CVE-2	019-14	372				
Libreoffice										
libreoffice			-							
Improper Input Validation	17-07-2019	7.5	where that pr be exec docum mouse- typical LibreLo turtle v which o	a featur nts can s ed scrip various ts such c. Libre(undled ogramn aphics s anipula rary pyt	specify ts can as Office is with nable script, ted into	w.libr e.org, t- us/se /advi /CVE·	e//ww reoffic /abou curity sories - -9848	A-LIB-L 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			commands. By using the document event feature to trigger LibreLogo to execute python contained within a document a malicious document could be constructed which would execute arbitrary python commands silently without warning. In the fixed versions, LibreLogo cannot be called from a document event handler. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5. CVE ID : CVE-2019-9848					
Informatio n Exposure	17-07-2019	4	LibreOffice has a 'stealth mode' in which only documents from locations deemed 'trusted' are allowed to retrieve remote resources. This mode is not the default mode, but can be enabled by users who want to disable LibreOffice's ability to include remote resources within a document. A flaw existed where bullet graphics were omitted from this protection prior to version 6.2.5. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5.	https://ww w.libreoffic e.org/abou t- us/security /advisories /CVE- 2019-9849	A-LIB-LIBR- 130819/156			
libsdl libsdl				1				
Out-of- bounds	16-07-2019	6.8	B SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x N/A A-LIB-LIBS- 130819/157					
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	C ID	
Read			buffer o video/s called f		d in Blit _N.c wh L_SoftBl					
			CVE ID	: CVE-2	019-13					
Libssh2			<u> </u>				<u> </u>		<u> </u>	
libssh2										
Integer Overflow or Wraparou nd	16-07-2019	5.8	In libssh2 before 1.9.0, kex_method_diffie_hellman_gr oup_exchange_sha256_key_exc hange in kex.c has an integer overflow that could lead to an out-of-bounds read in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. This is related to an _libssh2_check_length mistake, and is different from the various issues fixed in 1.8.1, such as CVE-2019-3855. CVE ID : CVE-2019-13115		N/A		A-LIB-L 130819			
linagora										
hublin										
Improper Limitation of a Pathname to a Restricted Directory ('Path	23-07-2019	5	LINAGORA hublin latest (commit 72ead897082403126bf8df926 4e70f0a9de247ff) is affected by: Directory Traversal. The impact is: The vulnerability allows an attacker to access any file (with a fixed extension) on the server. The				N/A		A-LIN-H 130819	
CV Scoring So	cale 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	Pa	tch	NCIIF	PC ID
Traversal')			component is: A web-view renderer; details here: https://lgtm.com/projects/g/l inagora/hublin/snapshot/af9f 1ce253b4ee923ff8da8f9d908d 02a8e95b7f/files/backend/we bserver/views.js?sort=name& dir=ASC&mode=heatmap&sho wExcluded=false#xb24eb0101 d2aec21:1. The attack vector is: Attacker sends a specially crafted HTTP request. CVE ID : CVE-2019-1010205							
Llnl										
model_spec	ific_registers-	safe								
Improper Access Control	18-07-2019	5	Labora affected Contro attacke specific compo The att attacke ioctl in checkin model normal for the versior	Lawrence Livermore National Laboratory msr-safe v1.1.0 is affected by: Incorrect Access Control. The impact is: An attacker could modify model specific registers. The component is: ioctl handling. The attack vector is: An attacker could exploit a bug in ioctl interface whitelist checking, in order to write to model specific registers, normally a function reserved for the root user. The fixed version is: v1.2.0. CVE ID : CVE-2019-1010066		N/A		A-LLN- 130819		
lodash										
lodash Uncontroll ed Resource Consumpti on	17-07-2019	4	lodash prior to 4.17.11 is affected by: CWE-400: Uncontrolled Resource Consumption. The impact is: Denial of service. The component is: Date handler.				N/A		A-LOD- 130819	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4 53	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	•					tch	NCIIP	CID
			The attac provides which th match us expression is: 4.17.1	very lo e librai sing a r on. The	ong stri ry atten egular	ngs, 1pts to				
			CVE ID :	CVE-2	019-10	10266				
logmeininc									<u> </u>	
join.me										
Improper Input Validation	17-07-2019	9.3	In LogMe 3.16.0.55 execute a on a targ vulnerab search pa application in Windo exploit th convincin follow an Successful cause the libraries targeted attacker behavior comman- the privil user if th crafted li that is ac vulnerab CVE ID :	505, an arbitran eted sy ility is aths us on URI ows. An nis vuln nis vuln nis vuln nalicio ul explo e applio from the could u to exe ds on t leges o e attac brary i ccessibl ole syste	attacke cy comm rstem. T due to m ed by th that is attacked nerabili rgeted u bus link. Ditation tation to he direct URI link use this cute ark he system f the tan ker can n a direct e to the em.	er could nands his unsafe ne defined er could ty by user to could o load ctory k. The pitrary em with rgeted place a ectory	N/A		A-LOG- 130819	
mailcleaner										
Informatio n Exposure	18-07-2019	5	MailCleaner before c888fbb6aaa7c5f8400f637bcf 1cbb844de46cd9 is affected by: Unauthenticated MySQL				N/A		A-MAI-1 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	CID
			database password information disclosure. The impact is: MySQL database content disclosure (e.g. username, password). The component is: The API call in the function allowAction() in NewslettersController.php. The attack vector is: HTTP Get request. The fixed version is: c888fbb6aaa7c5f8400f637bcf 1cbb844de46cd9. CVE ID : CVE-2019-1010246							
marginalia_	nnoiost		CVEID	: CVE-2	019-10	10246				
marginalia	project									
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	24-07-2019	7.5	SQL Inj The im SQL qu control as a con composi that ad user co parame attack v a SQL t vector(etc). Th	marginalia < 1.6 is affected by: SQL Injection. The impact is: The impact is a injection of any SQL queries when a user controller argument is added as a component. The component is: Affects users that add a component that is user controller, for instance a parameter or a header. The attack vector is: Hacker inputs a SQL to a vulnerable vector(header, http parameter, etc). The fixed version is: 1.6. CVE ID : CVE-2019-1010191		N/A		A-MAR- MARG- 130819		
Mcafee										
agent										
N/A	18-07-2019	4.6	Privilege escalation vulnerability in McAfee Agent (MA) before 5.6.1 HF3, allows local administrator users to potentially disable some McAfee processes by manipulating the MA directory			https: mcafe m/con te/ind age=c t&id=	e.co rpora lex?p onten	A-MCA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	•				tch	NCIIP	CID
			control and pl constructed fi directory.	e	•	288			
			CVE ID : CVE-	2019-35	92				
data_loss_p	revention_end	point							
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	24-07-2019	4.3	Improper New Input During V Generation ('O Scripting') in o McAfee Data I (DLPe) for Wi to 11.3.0 allow unauthenticat to trigger spec JavaScript to r UI via a carefu upload to a re which is corre DLPe Web Pro would then re when the DLP the event in th CVE ID : CVE-	https: mcafe m/con te/inc age=c t&id= 289	e.co rpora lex?p onten	A-MCA- 130819			
Improper Access Control	24-07-2019	4.6	Files or Direct to External Pa Data Loss Pre- for Windows 1 11.3.0 allows 1 user to redire to arbitrary lo incorrect acce applied to the allowing privi create symbol CVE ID : CVE-	https: mcafe m/con te/inc age=c t&id= 290	e.co rpora lex?p onten	A-MCA- 130819			
Metinfo									
metinfo									
Improper	19-07-2019	6.5	Metinfo 6.x all	lows SQL		N/A		A-MET-	METI-
CV Scoring So (CVSS)	cale 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
Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')			Injection via the id parameter in an admin/index.php?n=ui_set&m =admin&c=index&a=doget_tex t_content&table=lang&field=1 request. CVE ID : CVE-2019-13969					130819	/168	
Microsoft							1		1	
powershell	_core									
N/A	19-07-2019	1.9	vulnera Windov Applica which o to bypa aka 'Wi Applica Feature	rity featu ability ex ation Cor could allo ass WDA indows I ation Cor e Bypass : CVE-2	kists in ider introl (W ow an a C enford Defende introl Sec Vulnera	DAC) ttacker cement, r curity ability'.	N/A		A-MIC-F 130819	
microstrate	gy									
microstrate	gy_web									
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	10.4.6, metric validat	oStrateg there is a due to ir ion. • : CVE-2	stored X Isufficie	KSS in nt input	N/A		A-MIC-N 130819	
Modx										
modx_revol	ution									
Unrestricte d Upload of File with Dangerous	23-07-2019	5	MODX Revolution Gallery 1.7.0 is affected by: CWE-434: Unrestricted Upload of File with Dangerous Type. The				N/A		A-MOD- MODX- 130819	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Туре			impact is: Creating file with custom a filename and content. The component is: Filtering user parameters before passing them into phpthumb class. The attack vector is: web request via /assets/components/gallery/c onnector.php. CVE ID : CVE-2019-1010123		
Moinejf					
abcm2ps					
Improper Access Control	18-07-2019	4.3	moinejf abcm2ps 8.13.20 is affected by: Incorrect Access Control. The impact is: Allows attackers to cause a denial of service attack via a crafted file. The component is: front.c, function txt_add. The fixed version is: after commit commit 08aef597656d065e86075f3d5 3fda89765845eae. CVE ID : CVE-2019-1010069	N/A	A-MOI-ABCM- 130819/172
momo_proj	ect				
momo					
N/A	22-07-2019	4	The Momo application 2.1.9 for Android stores confidential information insecurely on the system (i.e., in cleartext), which allows a non-root user to find out the username/password of a valid user and a user's access token via Logcat. CVE ID : CVE-2019-13099	N/A	A-MOM- MOMO- 130819/173
Mozilla					

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

L

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	CID
firefox			1							
Use After Free	23-07-2019	7.5	can occ XMLHt event l main tl it has b in a po crash. ' affects Firefox 60.7.	after-free cur when tpReque oop, cau hread to been free tentially This vulu This vulu Thunde c < 67, ar	n workir est (XHR sing the be calle ed. This exploita nerabilit rbird < 0 nd Firefo	ng with) in an XHR d after cesults able y 50.7, ox ESR <	N/A		A-MOZ- 130819	
Use After Free	23-07-2019	7.5	can occ remove listene use, res exploit vulner Thund 67, and	l Firefox	n listene the ever er while n a pote sh. This ffects 60.7, Fi ESR < 6	rs are at still in ntially refox < 0.7.	N/A		A-MOZ- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	WebGI buffer graphic could r conten trigger exploit issue o Other o unaffeo affects Firefox 60.7.	Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-11692 The bufferdata function in WebGL is vulnerable to a buffer overflow with specific graphics drivers on Linux. This could result in malicious content freezing a tab or triggering a potentially exploitable crash. *Note: this issue only occurs on Linux. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-11693					A-MOZ- 130819	
Informatio	23-07-2019	5	A vulnerability exists in the				N/A		A-MOZ-	FIRE-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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 Exposure			Windows sandbox where an uninitialized value in memory can be leaked to a renderer from a broker when making a call to access an otherwise unavailable file. This results in the potential leaking of information stored at that memory location. *Note: this issue only occurs on Windows. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-11694		130819/177
Improper Input Validation	23-07-2019	4.3	A custom cursor defined by scripting on a site can position itself over the addressbar to spoof the actual cursor when it should not be allowed outside of the primary web content area. This could be used by a malicious site to trick users into clicking on permission prompts, doorhanger notifications, or other buttons inadvertently if the location is spoofed over the user interface. This vulnerability affects Firefox < 67. CVE ID : CVE-2019-11695	N/A	A-MOZ-FIRE- 130819/178
Improper Input Validation	23-07-2019	6.8	Files with the .JNLP extension used for "Java web start" applications are not treated as executable content for download prompts even though they can be executed if Java is installed on the local system. This could allow users	N/A	A-MOZ-FIRE- 130819/179
CV Scoring So (CVSS)	cale 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	ſ	Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
				execut	akenly l able bina ability af	ary local	ly. This				
				CVE ID) : CVE-2	019-11	696				
Improper Input Validation	23-07-20	019	4.3	pressed extensi the ext without delay t visible accept installa page co spoofin users in malicio vulnera 67.	ion insta ension v it the ins hat keep in order or declin ation. A n ould use ng on the nto insta ous exter ability at	users realistion p vill be in tall proposed to the pro- for use ne the naliciou this wit page to alling a nsion. The ffects Fin	ceive an prompt, estalled mpt ompt rs to s web h o trick nis cefox <	N/A		A-MOZ- 130819	
Improper Input Validation	23-07-20)19	5	dragge bookm the res subseq droppe area, an user's l run and conten data. T of brow malicio vulnera Thund 67, and	CVE ID : CVE-2019-11697 If a crafted hyperlink is dragged and dropped to the bookmark bar or sidebar and the resulting bookmark is subsequently dragged and dropped into the web content area, an arbitrary query of a user's browser history can be run and transmitted to the content page via drop event data. This allows for the theft of browser history by a malicious site. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-11698		N/A		A-MOZ- 130819		
Improper	23-07-20)19	4.3	A malio	cious pa	ge can b	riefly	N/A		A-MOZ-	FIRE-
CV Scoring So (CVSS)	cale 0-	-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			cause the wrong name to be highlighted as the domain name in the addressbar during page navigations. This could result in user confusion of which site is currently loaded for spoofing attacks. This vulnerability affects Firefox < 67. CVE ID : CVE-2019-11699		130819/182
Informatio n Exposure	23-07-2019	4.3	A hyperlink using the res: protocol can be used to open local files at a known location in Internet Explorer if a user approves execution when prompted. *Note: this issue only occurs on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 67. CVE ID : CVE-2019-11700	N/A	A-MOZ-FIRE- 130819/183
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-07-2019	4.3	The default webcal: protocol handler will load a web site vulnerable to cross-site scripting (XSS) attacks. This default was left in place as a legacy feature and has now been removed. *Note: this issue only affects users with an account on the vulnerable service. Other users are unaffected.*. This vulnerability affects Firefox < 67. CVE ID : CVE-2019-11701	N/A	A-MOZ-FIRE- 130819/184
Informatio n Exposure	23-07-2019	4.3	A hyperlink using protocols associated with Internet Explorer, such as IE.HTTP:, can be used to open local files at a known location with Internet	N/A	A-MOZ-FIRE- 130819/185

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				62						

Weakness	Publish Date	CVSS	I	Descriptic	n & CVE	ID	Pa	tch	NCIIP	C ID
			execut *Note: on Wir system	er if a us ion when this issu idows. O is are un ability af	n promp e only o ther ope affected	oted. ccurs erating .*. This				
			CVE ID) : CVE-2	019-11	702				
Incorrect Type Conversion or Cast	23-07-2019	7.5	can occ JavaSci issues allow f We are attacks flaw. T Firefox 67.0.3, 60.7.2.	his vulno ESR < 6 and Thu	n manip cts due pop. Th ploitable of target vild abus erability 0.7.1, Fi	ulating to is can e crash. ed sing this affects refox < rd <	N/A		A-MOZ- 130819	
						707				
Improper Input Validation	23-07-2019	10	CVE ID : CVE-2019-11707 Insufficient vetting of parameters passed with the Prompt:Open IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities this could result in executing arbitrary code on the user's computer. This vulnerability affects Firefox ESR < 60.7.2, Firefox < 67.0.4, and Thunderbird < 60.7.2. CVE ID : CVE-2019-11708		N/A		A-MOZ- 130819			
Improper Restriction	23-07-2019	7.5	Mozilla developers and community members reported				N/A		A-MOZ- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	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
of Operations within the Bounds of a Memory Buffer			memory safety bugs present in Firefox 67 and Firefox ESR 60.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. CVE ID : CVE-2019-11709				
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 67. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 68. CVE ID : CVE-2019-11710	N/A		A-MOZ- 130819	
Improper Input Validation	23-07-2019	6.8	When an inner window is reused, it does not consider the use of document.domain for cross-origin protections. If pages on different subdomains ever cooperatively use document.domain, then either page can abuse this to inject script into arbitrary pages on the other subdomain, even those that did not use document.domain to relax their origin security. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.	N/A		A-MOZ- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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-2019-11711		
Cross-Site Request Forgery (CSRF)	23-07-2019	6.8	POST requests made by NPAPI plugins, such as Flash, that receive a status 308 redirect response can bypass CORS requirements. This can allow an attacker to perform Cross- Site Request Forgery (CSRF) attacks. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. CVE ID : CVE-2019-11712	N/A	A-MOZ-FIRE- 130819/191
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in HTTP/2 when a cached HTTP/2 stream is closed while still in use, resulting in a potentially exploitable crash. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. CVE ID : CVE-2019-11713	N/A	A-MOZ-FIRE- 130819/192
Improper Input Validation	23-07-2019	7.5	Necko can access a child on the wrong thread during UDP connections, resulting in a potentially exploitable crash in some instances. This vulnerability affects Firefox < 68. CVE ID : CVE-2019-11714	N/A	A-MOZ-FIRE- 130819/193
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	23-07-2019	4.3	Due to an error while parsing page content, it is possible for properly sanitized user input to be misinterpreted and lead to XSS hazards on web sites in certain circumstances. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and	N/A	A-MOZ-FIRE- 130819/194
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIP	PC ID
Scripting')			Thunderbird < 60.8.				
			CVE ID : CVE-2019-11715				
Improper Input Validation	23-07-2019	5	A vulnerability exists where the caret ("^") character is improperly escaped constructing some URIs due to it being used as a separator, allowing for possible spoofing of origin attributes. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.	aret ("^") character is operly escaped ructing some URIs due to ng used as a separator, ing for possible spoofing gin attributes. This rability affects Firefox 60.8, Firefox < 68, and derbird < 60.8. D : CVE-2019-11717 importing a curve25519 te key in PKCS#8format eading 0x00 bytes, it is ole to trigger an out-of- ds read in the Network ity Services (NSS) library. could lead to information sure. This vulnerability			FIRE- /195
Out-of- bounds Read	23-07-2019	5	when importing a curve25519 private key in PKCS#8format with leading 0x00 bytes, it is possible to trigger an out-of- bounds read in the Network Security Services (NSS) library. This could lead to information disclosure. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. CVE ID : CVE-2019-11719	N/A		A-MOZ- 130819	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-07-2019	4.3	Some unicode characters are incorrectly treated as whitespace during the parsing of web content instead of triggering parsing errors. This allows malicious code to then be processed, evading cross- site scripting (XSS) filtering. This vulnerability affects Firefox < 68. CVE ID : CVE-2019-11720	N/A		A-MOZ- 130819	
Improper Input	23-07-2019	4.3	The unicode latin 'kra' character can be used to spoof a standard 'k' character in the	N/A		A-MOZ- 130819	
CV Scoring So (CVSS)	cale 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	NCIIF	PC ID	
Validation				domai not dis allowin	sbar. Th n spoofir play as p ng for us 1lnerabil c < 68.	ng attack ounycod er confu	xs as do e text, sion.					
				CVE IE) : CVE-2	019-11	721					
Informatio n Exposure	23-07-2	2019	5	the ins where the ori brows leak co brows differe people Multi-A Extens	erability tallation the initi- gin attri- ing conte- ookies in ing mode nt "conta who use Account ion. This Firefox	of add- al fetch i butes of ext. This private e or acro ainers" f e the Fir Containe s vulnera	ons ignored the could oss for efox ers Web	N/A		A-MOZ- 130819		
				CVE IE) : CVE- 2	019-11	723					
Improper Input Validation	23-07-2	2019	4	When a user navigates to site marked as unsafe by the Safebrowsing API, warning messages are displayed and navigation is interrupted but resources from the same site loaded through websockets are not blocked, leading to the loading of unsafe resources and bypassing safebrowsing protections. This vulnerability affects Firefox < 68. CVE ID : CVE-2019-11725				N/A		A-MOZ- 130819		
Improper Certificate Validation	23-07-2	2019	5	possib Securi Certific v1.5 si	erability le to forc ty Servic cateVerif gnatures ly ones a	e Netwo es (NSS) by with F when t	ork) to sign PKCS#1 hose are	N/A		A-MOZ-FIRE- 130819/201		
CV Scoring Se	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

C	/ Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
					C7						

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	CID
			TLS 1.3 signatu for TLS	in Certif 3. PKCS# 1res sho 5 1.3 mes ability at	1 v1.5 uld not ssages. 7	Гhis				
			CVE ID) : CVE-2	2019-11	727				
Improper Input Validation	23-07-2019	4.3	header a malic ports c accessi conten vulner 68.	, Alt-Svo cious site of any ho ble to a t is load ability at	c, can be e to scan ost that t user wh ed. This ffects Fi	en web refox <	N/A		A-MOZ- 130819	
Improper Input Validation	23-07-2019	5	Empty ECDH J a segm values sanitiz into ma vulner ESR < 0	CVE ID : CVE-2019-11728 Empty or malformed p256- ECDH public keys may trigger a segmentation fault due values being improperly sanitized before being copied into memory and used. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.					A-MOZ- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	commu memor Firefox and Th these b memor presum effort t be expl code. T Thund	bugs pr efox ESR and 60.6. wed evi ption an vith eno e of the run arb	reported resent in 60.6, Some of dence of d we ugh se could bitrary y affects refox <			A-MOZ- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Improper Restriction of Operations within the Bounds of a Memory Buffer23-07-20197.5Mozilla developers and community members reported memory safety bugs present in Firefox 66. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 67.N/AA-MOZ-FIRE- 130819/206Concurrent Execution within the Bounds of a Memory23-07-20197.5If hyperthreading is not disabled, a timing attack vulnerability exists, similar to previous Spectre attacks. Apple has shipped macOS 10.14.5 with an option to disable hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker threads. *Note: users need to update to macOS 10.14.5 in order to take advantage of thisN/AA-MOZ-FIRE- 130819/206Concurrent (Race Condition')23-07-20196.8If hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker threads. *Note: users need to update to macOS 10.14.5 in order to take advantage of thisN/AA-MOZ-FIRE- 130819/207	Weakness	Publish Date	CVSS	[Descriptio	on & CVE	Pat	tch	NCIIF	PC ID	
N/A23-07-20195.1entry, a researcher demonstrated a sandbox escape by installing a malicious language pack and then opening a browser feature that used the compromised translation. This vulnerability affects Firefox 60.8. CVE ID : CVE-2019-9811N/AA-M0Z-FIRE- 130819/205Improper Restriction of Operations within the Bounds of a Memory BufferZ3-07-20197.5Mozilla developers and community members reported memory safety bugs present in Firefox 66. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 67. CVE ID : CVE-2019-9814N/AA-M0Z-FIRE- 130819/206Concurrent Essecution using Shared Resource with in mproper Synchroniz ation (Race Condition)If hyperthreading is not disable hyperthreading in applications runing uplications runing applications runing update to macOS 10.14.5 in ord to take advantage of thisN/AA-M0Z-FIRE- 130819/206				CVE ID) : CVE-2	019-98	00				
Improper Restriction of Operations within the Bounds of a Memory Buffer23-07-20197.5community members reported memory safety bugs present in Firefox 66. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 67.N/AA-MOZ-FIRE- 130819/206Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')If hyperthreading is not disable d, a timing attack vulnerability exists, similar to previous Spectre attacks. Apple has shipped macOS 10.14.5 with an option to disable hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker threads. *Note: users need to update to macOS 10.14.5 in order to take advantage of thisN/AA-MOZ-FIRE- 130819/207	N/A	23-07-2019	5.1	entry, a demon escape malicio then op feature compro vulnera ESR < 6 Thundo	a researc strated a by insta ous langu pening a e that use omised t ability af 60.8, Fire erbird <	ther a sandbo lling a lage pao browse ed the ranslati fects Fin efox < 68 60.8.	ox ek and r on. This refox 8, and	N/A		_	
Concurrent Execution using Shared Resource with 123-07-2019disabled, a timing attack vulnerability exists, similar to previous Spectre attacks. Apple has shipped macOS 10.14.5 with an option to disable hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker Condition')A-MOZ-FIRE- 130819/207OV Scoring Scale0.14.5 with an option to disable hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker threads. *Note: users need to update to macOS 10.14.5 in order to take advantage of thisN/AA-MOZ-FIRE- 130819/207	Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	commu memor Firefox showed corrup that wi some o exploit code. T Firefox	mbers r bugs pr he of the ce of me we pres gh effort could be n arbitra erability	eported resent in rese bugs emory sume t that ary y affects	N/A				
		23-07-2019	6.8	disable vulnera previou Apple I 10.14.5 disable applica untrus throug now m main th thread update	ng attac kists, sin re attacl bed mac option nreading nning in a thr sysctl. F of it on d any w users n OS 10.14	k nilar to ks. OS to g in ead firefox the forker eed to k.5 in	N/A				
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	-	cale 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	Pat	tch	NCIIF	PC ID	
				affects	e.*. This v Thunde < < 67, ar	rbird < 6					
				CVE IE) : CVE- 2	019-98	15				
Incorrect Type Conversion or Cast	23-07-2	2019	4.3	where occury JavaSc groups bypass within this vu been d Unbox disable suppor vulner Thund 67, and	erability infusion c inipulati cts in ob g for the curity c oups. *N ity has o rated with ts, which fault on a ases.*. T ffects 60.7, Fin ESR < 6	an ng oject e hecks lote: nly ch are all his cefox < 0.7.	N/A		A-MOZ- 130819		
Origin Validation Error	23-07-2	2019	5	domai canvas circum used to differe same-o vulner Thund 67, and	Images from a different domain can be read using a canvas object in some circumstances. This could be used to steal image data from a different site in violation of same-origin policy. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-9817					A-MOZ- 130819	
Improper Input Validation	23-07-2	2019	7.5	JavaSc misma workin resulti exploit	erability ript com tch can o ng with t ng in a p table cra ability at	partmer occur wł he fetch otential sh. This	nt nile API,	N/A		A-MOZ-FIRE- 130819/210	
CV Scoring So	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				70						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-9819		
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in the chrome event handler when it is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-9820	N/A	A-MOZ-FIRE- 130819/211
Use After Free	23-07-2019	6.8	A use-after-free vulnerability can occur in AssertWorkerThread due to a race condition with shared workers. This results in a potentially exploitable crash. This vulnerability affects Firefox < 67. CVE ID : CVE-2019-9821	N/A	A-MOZ-FIRE- 130819/212
firefox_esr					
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur when working with XMLHttpRequest (XHR) in an event loop, causing the XHR main thread to be called after it has been freed. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.	N/A	A-MOZ-FIRE- 130819/213
			CVE ID : CVE-2019-11691 A use-after-free vulnerability		
Use After Free	23-07-2019	7.5	can occur when listeners are removed from the event listener manager while still in	N/A	A-MOZ-FIRE- 130819/214

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				71						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.		
			CVE ID : CVE-2019-11692		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	The bufferdata function in WebGL is vulnerable to a buffer overflow with specific graphics drivers on Linux. This could result in malicious content freezing a tab or triggering a potentially exploitable crash. *Note: this issue only occurs on Linux. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-11693	N/A	A-MOZ-FIRE- 130819/215
Informatio n Exposure	23-07-2019	5	A vulnerability exists in the Windows sandbox where an uninitialized value in memory can be leaked to a renderer from a broker when making a call to access an otherwise unavailable file. This results in the potential leaking of information stored at that memory location. *Note: this issue only occurs on Windows. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-11694	N/A	A-MOZ-FIRE- 130819/216
Improper	23-07-2019	5	If a crafted hyperlink is	N/A	A-MOZ-FIRE-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			dragged and dropped to the bookmark bar or sidebar and the resulting bookmark is subsequently dragged and dropped into the web content area, an arbitrary query of a user's browser history can be run and transmitted to the content page via drop event data. This allows for the theft of browser history by a malicious site. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.		130819/217
			CVE ID : CVE-2019-11698		
Incorrect Type Conversion or Cast	23-07-2019	7.5	A type confusion vulnerability can occur when manipulating JavaScript objects due to issues in Array.pop. This can allow for an exploitable crash. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Firefox ESR < 60.7.1, Firefox < 67.0.3, and Thunderbird < 60.7.2.	N/A	A-MOZ-FIRE- 130819/218
			CVE ID : CVE-2019-11707		
Improper Input Validation	23-07-2019	10	Insufficient vetting of parameters passed with the Prompt:Open IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities this could result in executing arbitrary code on the user's	N/A	A-MOZ-FIRE- 130819/219
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			computer. This vulnerability affects Firefox ESR < 60.7.2, Firefox < 67.0.4, and Thunderbird < 60.7.2.		
			CVE ID : CVE-2019-11708		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 67 and Firefox ESR 60.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.	N/A	A-MOZ-FIRE- 130819/220
			CVE ID : CVE-2019-11709		
Improper Input Validation	23-07-2019	6.8	When an inner window is reused, it does not consider the use of document.domain for cross-origin protections. If pages on different subdomains ever cooperatively use document.domain, then either page can abuse this to inject script into arbitrary pages on the other subdomain, even those that did not use document.domain to relax their origin security. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.	N/A	A-MOZ-FIRE- 130819/221
			CVE ID : CVE-2019-11711		
Cross-Site Request Forgery	23-07-2019	6.8	POST requests made by NPAPI plugins, such as Flash, that receive a status 308 redirect	N/A	A-MOZ-FIRE- 130819/222

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
34										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			response can bypass CORS requirements. This can allow an attacker to perform Cross- Site Request Forgery (CSRF) attacks. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.		
			CVE ID : CVE-2019-11712		
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in HTTP/2 when a cached HTTP/2 stream is closed while still in use, resulting in a potentially exploitable crash. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.	N/A	A-MOZ-FIRE- 130819/223
			CVE ID : CVE-2019-11713		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-07-2019	4.3	Due to an error while parsing page content, it is possible for properly sanitized user input to be misinterpreted and lead to XSS hazards on web sites in certain circumstances. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. CVE ID : CVE-2019-11715	N/A	A-MOZ-FIRE- 130819/224
Improper Input Validation	23-07-2019	5	A vulnerability exists where the caret ("^") character is improperly escaped constructing some URIs due to it being used as a separator, allowing for possible spoofing of origin attributes. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.	N/A	A-MOZ-FIRE- 130819/225
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIF	PC ID
			CVE ID) : CVE-2	019-11	717				
Out-of- bounds Read	23-07-2019	5	private with le possibl bounds Securit This co disclos affects Firefox < 60.8.	e key in F eading 0x le to trig s read in ty Servic ould lead sure. This Firefox 1 x < 68, an	PKCS#81 200 byte ger an o the Net es (NSS) to infor s vulner ESR < 60 nd Thun	es, it is out-of- work) library. mation ability 0.8, derbird	N/A		A-MOZ- 130819	
Improper Input Validation	23-07-2019	5	CVE ID : CVE-2019-11719Empty or malformed p256-ECDH public keys may triggera segmentation fault duevalues being improperlysanitized before being copiedinto memory and used. Thisvulnerability affects FirefoxESR < 60.8, Firefox < 68, and				N/A		A-MOZ- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 66, Firefox ESR 60.6, and Thunderbird 60.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-9800				N/A		A-MOZ- 130819	
N/A	23-07-2019	5.1	As part of a winning Pwn2Own entry, a researcher			N/A		A-MOZ- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 76	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			demonstrated a sandbox escape by installing a malicious language pack and then opening a browser feature that used the compromised translation. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. CVE ID : CVE-2019-9811				
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	23-07-2019	6.8	If hyperthreading is not disabled, a timing attack vulnerability exists, similar to previous Spectre attacks. Apple has shipped macOS 10.14.5 with an option to disable hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker threads. *Note: users need to update to macOS 10.14.5 in order to take advantage of this change.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-9815	N/A		A-MOZ- 130819	
Incorrect Type Conversion or Cast	23-07-2019	4.3	A possible vulnerability exists where type confusion can occur when manipulating JavaScript objects in object groups, allowing for the bypassing of security checks within these groups. *Note: this vulnerability has only been demonstrated with UnboxedObjects, which are	N/A		A-MOZ- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disabled by default on all supported releases.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.		
			CVE ID : CVE-2019-9816		
Origin Validation Error	23-07-2019	5	Images from a different domain can be read using a canvas object in some circumstances. This could be used to steal image data from a different site in violation of same-origin policy. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.	N/A	A-MOZ-FIRE- 130819/232
			CVE ID : CVE-2019-9817		
Improper Input Validation	23-07-2019	7.5	A vulnerability where a JavaScript compartment mismatch can occur while working with the fetch API, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.	N/A	A-MOZ-FIRE- 130819/233
			CVE ID : CVE-2019-9819		
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in the chrome event handler when it is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-9820	N/A	A-MOZ-FIRE- 130819/234
thunderbird	d		I		
Use After	23-07-2019	7.5	A use-after-free vulnerability	N/A	A-MOZ-
CV Scoring So (CVSS)	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
Free			can occur when working with XMLHttpRequest (XHR) in an event loop, causing the XHR main thread to be called after it has been freed. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-11691		THUN- 130819/235		
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur when listeners are removed from the event listener manager while still in use, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-11692	N/A	A-MOZ- THUN- 130819/236		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	The bufferdata function in WebGL is vulnerable to a buffer overflow with specific graphics drivers on Linux. This could result in malicious content freezing a tab or triggering a potentially exploitable crash. *Note: this issue only occurs on Linux. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-11693	N/A	A-MOZ- THUN- 130819/237		
Informatio n Exposure	23-07-2019	5	A vulnerability exists in the Windows sandbox where an uninitialized value in memory	N/A	A-MOZ- THUN- 130819/238		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			can be leaked to a renderer from a broker when making a call to access an otherwise unavailable file. This results in the potential leaking of information stored at that memory location. *Note: this issue only occurs on Windows. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-11694			
Improper Input Validation	23-07-2019	5	If a crafted hyperlink is dragged and dropped to the bookmark bar or sidebar and the resulting bookmark is subsequently dragged and dropped into the web content area, an arbitrary query of a user's browser history can be run and transmitted to the content page via drop event data. This allows for the theft of browser history by a malicious site. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-11698	N/A	A-MOZ- THUN- 130819/239	
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	A flaw in Thunderbird's implementation of iCal causes a heap buffer overflow in parser_get_next_char when processing certain email messages, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7.1.	N/A	A-MOZ- THUN- 130819/240	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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-2019-11703		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	A flaw in Thunderbird's implementation of iCal causes a heap buffer overflow in icalmemory_strdup_and_dequ ote when processing certain email messages, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7.1. CVE ID : CVE-2019-11704	N/A	A-MOZ- THUN- 130819/241
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	A flaw in Thunderbird's implementation of iCal causes a stack buffer overflow in icalrecur_add_bydayrules when processing certain email messages, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7.1. CVE ID : CVE-2019-11705	N/A	A-MOZ- THUN- 130819/242
Incorrect Type Conversion or Cast	23-07-2019	5	A flaw in Thunderbird's implementation of iCal causes a type confusion in icaltimezone_get_vtimezone_p roperties when processing certain email messages, resulting in a crash. This vulnerability affects Thunderbird < 60.7.1. CVE ID : CVE-2019-11706	N/A	A-MOZ- THUN- 130819/243
Incorrect Type Conversion or Cast	23-07-2019	7.5	A type confusion vulnerability can occur when manipulating JavaScript objects due to issues in Array.pop. This can allow for an exploitable crash. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects	N/A	A-MOZ- THUN- 130819/244
CV Scoring So (CVSS)	cale 0-1	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 60.7.1, Firefox < 67.0.3, and Thunderbird < 60.7.2.		
			CVE ID : CVE-2019-11707		
Improper Input Validation	23-07-2019	10	Insufficient vetting of parameters passed with the Prompt:Open IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities this could result in executing arbitrary code on the user's computer. This vulnerability affects Firefox ESR < 60.7.2, Firefox < 67.0.4, and Thunderbird < 60.7.2. CVE ID : CVE-2019-11708	N/A	A-MOZ- THUN- 130819/245
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 67 and Firefox ESR 60.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. CVE ID : CVE-2019-11709	N/A	A-MOZ- THUN- 130819/246
Improper Input Validation	23-07-2019	6.8	When an inner window is reused, it does not consider the use of document.domain for cross-origin protections. If	N/A	A-MOZ- THUN- 130819/247

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
82											

Г

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		ever cooperatively use document.domain, then either page can abuse this to inject script into arbitrary pages on the other subdomain, even those that did not use document.domain to relax their origin security. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.			
Cross-Site Request Forgery (CSRF)	23-07-2019	6.8		N/A	A-MOZ- THUN- 130819/248
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in HTTP/2 when a cached HTTP/2 stream is closed while still in use, resulting in a potentially exploitable crash. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. CVE ID : CVE-2019-11713	N/A	A-MOZ- THUN- 130819/249
Improper Neutralizat ion of Input	23-07-2019	4.3	Due to an error while parsing page content, it is possible for properly sanitized user input to be misinterpreted and lead	N/A	A-MOZ- THUN- 130819/250

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				02						

Г

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	l	NCIIP	C ID
During Web Page Generation ('Cross-site Scripting')			to XSS hazards on web sites in certain circumstances. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.				
			CVE ID : CVE-2019-11715				
Improper Input Validation	23-07-2019	5	A vulnerability exists where the caret ("^") character is improperly escaped constructing some URIs due to it being used as a separator, allowing for possible spoofing of origin attributes. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.	N/A		A-MOZ- THUN- 130819	
			CVE ID : CVE-2019-11717				
Out-of- bounds Read	23-07-2019	5	When importing a curve25519 private key in PKCS#8format with leading 0x00 bytes, it is possible to trigger an out-of- bounds read in the Network Security Services (NSS) library. This could lead to information disclosure. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. CVE ID : CVE-2019-11719			A-MOZ- THUN- 130819	
Improper Input Validation	23-07-2019	5	Empty or malformed p256- ECDH public keys may trigger a segmentation fault due values being improperly sanitized before being copied into memory and used. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. CVE ID : CVE-2019-11729	N/A		A-MOZ- THUN- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 66, Firefox ESR 60.6, and Thunderbird 60.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-9800	N/A	A-MOZ- THUN- 130819/254
N/A	23-07-2019	5.1	As part of a winning Pwn2Own entry, a researcher demonstrated a sandbox escape by installing a malicious language pack and then opening a browser feature that used the compromised translation. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. CVE ID : CVE-2019-9811	N/A	A-MOZ- THUN- 130819/255
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	23-07-2019	6.8	If hyperthreading is not disabled, a timing attack vulnerability exists, similar to previous Spectre attacks. Apple has shipped macOS 10.14.5 with an option to disable hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker threads. *Note: users need to update to macOS 10.14.5 in	N/A	A-MOZ- THUN- 130819/256
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			order to take advantage of this change.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-9815		
Incorrect Type Conversion or Cast	23-07-2019	4.3	A possible vulnerability exists where type confusion can occur when manipulating JavaScript objects in object groups, allowing for the bypassing of security checks within these groups. *Note: this vulnerability has only been demonstrated with UnboxedObjects, which are disabled by default on all supported releases.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-9816	N/A	A-MOZ- THUN- 130819/257
Origin Validation Error	23-07-2019	5	Images from a different domain can be read using a canvas object in some circumstances. This could be used to steal image data from a different site in violation of same-origin policy. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. CVE ID : CVE-2019-9817	N/A	A-MOZ- THUN- 130819/258
Improper Input Validation	23-07-2019	7.5	A vulnerability where a JavaScript compartment mismatch can occur while working with the fetch API, resulting in a potentially exploitable crash. This	N/A	A-MOZ- THUN- 130819/259

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				00						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.			
			CVE ID : CVE-2019-9819			
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in the chrome event handler when it is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.	N/A	A-MOZ- THUN- 130819/260	
			CVE ID : CVE-2019-9820			
mpg321_pr	oject					
mpg321						
Out-of- bounds Write	24-07-2019	4.3	The scan() function in mad.c in mpg321 0.3.2 allows remote attackers to trigger an out-of- bounds write via a zero bitrate in an MP3 file. CVE ID : CVE-2019-14247	N/A	A-MPG-MPG3- 130819/261	
myt_projec	t					
myt						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	In MyT 1.5.1, the User[username] parameter has XSS. CVE ID : CVE-2019-13346	N/A	A-MYT-MYT- 130819/262	
nasa						
cfitsio						
Improper Restriction of	16-07-2019	7.5	NASA CFITSIO prior to 3.43 is affected by: Buffer Overflow. The impact is: arbitrary code	N/A	A-NAS-CFIT- 130819/263	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			execution. The component is: over 40 source code files were changed. The attack vector is: remote unauthenticated attacker. The fixed version is: 3.43. NOTE: this CVE refers to the issues not covered by CVE- 2018-3846, CVE-2018-3847, CVE-2018-3848, and CVE- 2018-3849. One example is ftp_status in drvrnet.c mishandling a long string beginning with a '4' character.		
			CVE ID : CVE-2019-1010060		
nevma					
adaptive_in	nages			Γ	-
Informatio n Exposure	21-07-2019	5	A Local File Inclusion vulnerability in the Nevma Adaptive Images plugin before 0.6.67 for WordPress allows remote attackers to retrieve arbitrary files via the \$REQUEST['adaptive-images- settings']['source_file'] parameter in adaptive-images- script.php. CVE ID : CVE-2019-14205	N/A	A-NEV-ADAP- 130819/264
Improper Input Validation	21-07-2019	6.4	An Arbitrary File Deletion vulnerability in the Nevma Adaptive Images plugin before 0.6.67 for WordPress allows remote attackers to delete arbitrary files via the \$REQUEST['adaptive-images- settings'] parameter in adaptive-images-script.php. CVE ID : CVE-2019-14206	N/A	A-NEV-ADAP- 130819/265
nfdump_pro	oject			<u> </u>	
CV Scoring So					

(CVSS)	01	12	23	3 4	4.5	50	07	7-0	0-9	5 10
CV Scoring Scale	0_1	1_2	2_2	2_1	4-5	5-6	6-7	7-8	8-0	9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
16-07-2019	6.8	nfdump 1.6.16 and earlier is affected by: Buffer Overflow. The impact is: The impact could range from a denial of service to local code execution. The component is: nfx.c:546, nffile_inline.c:83, minilzo.c (redistributed). The attack vector is: nfdump must read and process a specially crafted file. The fixed version is: after commit 9f0fe9563366f62a71d34c922 29da3432ec5cf0e. CVE ID : CVE-2019-1010057	N/A	A-NFD-NFDU- 130819/266
16-07-2019	4.3	njs through 0.3.3, used in NGINX, has a heap-based buffer over-read in nxt_vsprintf in nxt/nxt_sprintf.c during error handling, as demonstrated by an njs_regexp_literal call that leads to an njs_parser_lexer_error call and then an njs_parser_scope_error call. CVE ID : CVE-2019-13617	N/A	A-NGI-NJS- 130819/267
nanager				
16-07-2019	1.7	Norton Password Manager, prior to 6.3.0.2082, may be susceptible to an address spoofing issue. This type of issue may allow an attacker to disguise their origin IP address	https://sup port.syman tec.com/us /en/article. SYMSA148 3.html	A-NOR-PASS- 130819/268
		6 6		
	16-07-2019 16-07-2019	16-07-2019 6.8 16-07-2019 4.3 16-07-2019 4.3	16-07-20196.8Infdump 1.6.16 and earlier is affected by: Buffer Overflow. The impact is: The impact could range from a denial of service to local code execution. The component is: nfx.c:546, nffile_inline.c:83, minilzo.c (redistributed). The attack vector is: nfdump must read and process a specially crafted file. The fixed version is: after commit 9f0fe9563366f62a71d34c922 29da3432ec5cf0e. CVE ID : CVE-2019-101005716-07-20194.3njs through 0.3.3, used in NGINX, has a heap-based buffer over-read in nxt_vsprintf in nxt_nxt_sprintf.c during error handling, as demonstrated by an njs_parser_lexer_error call and then an njs_parser_lexer_error call and then an njs_parser_scope_error call. CVE ID : CVE-2019-1361716-07-20191.7Norton Password Manager, prior to 6.3.0.2082, may be susceptible to an address spoofing issue. This type of	16-07-2019Image: A second

Weakness	Publi	sh Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	PC ID
					er to obfu						
				source of network traffic. CVE ID : CVE-2019-9700							
				CVEID	: CVE-2	019-97	00				
NSA											
ghidra											
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-07	7-2019	6.8	where an intermediate analysis result is archived for sharing with other persons. To achieve arbitrary code execution, one approach is to overwrite some critical Ghidra modules, e.g., the decompile module. CVE ID : CVE-2019-13623		N/A		A-NSA-0 130819			
Improper Restriction of XML External Entity Reference ('XXE')	16-07	7-2019	9.4	NSA Ghidra before 9.0.1 allows XXE when a project is opened or restored, or a tool is imported, as demonstrated by a project.prp file. CVE ID : CVE-2019-13625			N/A		A-NSA-0 130819		
Offis											
dcmtk											
Improper Restriction of Operations within the	22-07	7-2019	7.5	OFFIS.de DCMTK 3.6.3 and below is affected by: Buffer Overflow. The impact is: Possible code execution and confirmed Denial of Service.			N/A		A-OFF-1 130819		
CV Scoring So (CVSS)	cale	0-1	1-2	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
Bounds of a Memory Buffer			The component is: DcmRLEDecoder::decompress () (file dcrledec.h, line 122). The attack vector is: Many scenarios of DICOM file processing (e.g. DICOM to image conversion). The fixed version is: 3.6.4, after commit 40917614e. CVE ID : CVE-2019-1010228				
oisf							
suricata							
Improper Input Validation	18-07-2019	5	Open Information Security Foundation Suricata prior to version 4.1.2 is affected by: Denial of Service - DNS detection bypass. The impact is: An attacker can evade a signature detection with a specialy formed network packet. The component is: app-layer-detect-proto.c, decode.c, decode-teredo.c and decode-ipv6.c (https://github.com/OISF/suri cata/pull/3590/commits/11f3 659f64a4e42e90cb3c09fcef66 894205aefe, https://github.com/OISF/suri cata/pull/3590/commits/835 7ef3f8ffc7d99ef65713507241 60de356158b). The attack vector is: An attacker can trigger the vulnerability by sending a specifically crafted network request. The fixed version is: 4.1.2. CVE ID : CVE-2019-1010251	N/A		A-0IS-S 130819	
onionbuzz				I			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
onionbuzz					
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-07-2019	7.5	An issue was discovered in the Viral Quiz Maker - OnionBuzz plugin before 1.2.7 for WordPress. One could exploit the id parameter in the set_count ajax nopriv handler due to there being no sanitization prior to use in a SQL query in saveQuestionVote. This allows an unauthenticated/unprivileged user to perform a SQL injection attack capable of remote code execution and information disclosure. CVE ID : CVE-2019-14230	N/A	A-ONI-ONIO- 130819/273
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	21-07-2019	7.5	An issue was discovered in the Viral Quiz Maker - OnionBuzz plugin before 1.2.2 for WordPress. One could exploit the points parameter in the ob_get_results ajax nopriv handler due to there being no sanitization prior to use in a SQL query in getResultByPointsTrivia. This allows an unauthenticated/unprivileged user to perform a SQL injection attack capable of remote code execution and information disclosure. CVE ID : CVE-2019-14231	N/A	A-ONI-ONIO- 130819/274
onosproject	t				
onos					
N/A	16-07-2019	10	In ONOS 1.15.0, apps/yang/web/src/main/jav	N/A	A-ONO-ONOS- 130819/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a/org/onosproject/yang/web /YangWebResource.java mishandles backquote characters within strings that can be used in a shell command.		
			CVE ID : CVE-2019-13624		
opensns					
opensns					
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	25-07-2019	6.5	OpenSNS v6.1.0 allows SQL Injection via the index.php?s=/ucenter/Config/ uid parameter because of the getNeedQueryData function in Application/Common/Model/ UserModel.class.php. CVE ID : CVE-2019-14266	N/A	A-OPE-OPEN- 130819/276
Oracle	<u> </u>			I	
retail_xstor	e_office				
Improper Access Control	23-07-2019	6.4	Vulnerability in the Oracle Retail Xstore Office component of Oracle Retail Applications (subcomponent: Internal Operations). Supported versions that are affected are 7.0 and 7.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Xstore Office. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Retail Xstore Office accessible data as well as unauthorized	N/A	A-ORA-RETA- 130819/277
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

bi_publisher			update, insert or delete access to some of Oracle Retail Xstore Office accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:U/C:H/I:L/A:N). CVE ID : CVE-2019-2561 Vulnerability in the BI		
bi_publisher			Vulnerability in the BI		
			Vulnerability in the BI		
Improper Access 2 Control	23-07-2019	6.4	Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). While the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data as well as unauthorized read access to a subset of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA-BI_P- 130819/278

6-7

8-9

9-10

7-8

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6
				94		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:C/C:L/I:L/A:N).		
			CVE ID : CVE-2019-2767		
Informatio n Exposure	23-07-2019	5	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:U/C:H/I:N/A:N).	N/A	A-ORA-BI_P- 130819/279
			CVE ID : CVE-2019-2768		
Improper Access Control	23-07-2019	6	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher	N/A	A-ORA-BI_P- 130819/280
CV Scoring So (CVSS)	cale 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	I	Descriptio	on & CVE	Pa	tch	NCIIP	CID	
				Succes human person and wh in BI P Publish signific produc this vu unauth deletio to criti Publish well as access Publish unauth partial (partia (forme CVSS 3 (Confic Availah Vector (CVSS: :R/S:C,	sful atta interac other the nile the v ublisher ner), atta cantly in cts. Succ lnerabil norized o n or mo cal data ner (forr ner) acce orized a denial o l DOS) o erly XML .0 Base 1 dentialit pility im : 3.0/AV:1	vulnerab (formen acks may apact ad essful at ity can r creation, dificatio or all BI nerly XM essible d orized r set of BI nerly XM essible d ability to of service of BI Pub Score 8.2 y, Integr pacts). C	attacker olity is oly XML ditional tacks of esult in n access AL ata as ead AL ata and cause a e lisher er). 2 otty and CVSS PR:L/UI				
solaris											
Improper Access Control	23-0	7-2019	4	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Automount). Supported versions that are affected are 11.4 and 10. Difficult to exploit vulnerability allows unauthenticated attacker with			N/A		A-ORA- 130819		
CV Scoring So (CVSS)	cale	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	Pa	tch	NCIIP	CID
			compre Success human person Success vulnera unauth delete Solaris as unau a subse accessi Score 4 Integri Vector (CVSS: I:R/S:U	sful atta ability ca acrized u access to accessif uthorize et of Ora ble data k.2 (Conf ty impace	racle Sol cks requ tion from nan the a cks of th pdate, i o some c ole data d read a cle Solan . CVSS 3 fidential cts). CVS	laris. hire n a attacker. his t in nsert or of Oracle as well ccess to ris .0 Base ity and S /PR:N/U				
Improper Access Control	23-07-2019	2.6	compo System (subco Tools). that is to expl unauth logon t where compro Success human person Success vulners unauth deletio to criti accessi unauth	oit vulne enticate o the inf Solaris e omise So sful atta other th sful atta ability ca dorized c n or mod cal data ble data	Dracle Si cts Suite t: Open oported is 11.4. erability d attack frastruct executes olaris. cks requi- tion from nan the a cks of the an result reation, dificatio or all So and bility to	un Fabrics Version Difficult allows ter with ture to iire n a attacker. is t in n access laris	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of Solaris. CVSS 3.0 Base Score 6.3 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/U I:R/S:U/C:N/I:H/A:H). CVE ID : CVE-2019-2788		
Improper Access Control	23-07-2019	4.6	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Common Desktop Environment). The supported version that is affected is 10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI :N/S:C/C:H/I:H/A:H). CVE ID : CVE-2019-2832	N/A	A-ORA-SOLA- 130819/283
Improper Access Control	23-07-2019	5	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). The supported version that is affected is 11.4. Easily exploitable vulnerability	N/A	A-ORA-SOLA- 130819/284
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	PC ID
			Solaris this vu unauth deletio to criti Solaris 3.0 Bas impact	access oracle cks of esult in n access cacle CVSS egrity PR:N/U						
Improper Access Control	23-07-2019	4.6	Solaris Sun Sys (subco Tools). that is a exploit allows with lo infrast Solaris compre While t Oracle signific produc this vu takeov CVSS 3 (Confic Availat Vectors (CVSS:: :N/S:C,	ability in compor- stems Pr mponen The sup affected able vul- low prive gon to the ructure ve comise Or the vulne Solaris, in cantly imports. Succe lnerabili er of Ora .0 Base S dentiality pility imports 3.0/AV:I /C:H/I:H	nent of C roducts t: LDAP oported is 11.4. nerabili rileged a ne where O s to racle Sol erability attacks n pact ad essful at ty can r acle Sola Score 8.8 y, Integr pacts). C	Dracle Suite Client version Easily ty ttacker racle aris. racle aris. ris in may ditional tacks of esult in aris. 3 ity and VSS PR:L/UI	N/A		A-ORA- 130819	
Improper	23-07-2019	6.9	Vulner	ability ir	the Ora	acle	N/A		A-ORA-	SOLA-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 99	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIF	PC ID
Access Control			Solaris component of Oracle Sun Systems Products Suite (subcomponent: Filesystem). Supported versions that are affected are 11.4 and 10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI :R/S:U/C:H/I:H/A:H). CVE ID : CVE-2019-2804			130819	9/286
Improper Access Control	23-07-2019	3.3	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Zones). The supported version that is affected is 11.4. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in	N/A		A-ORA- 130819	
CV Scoring So	cale 0-1	1-2	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	NCIIPC	ID
			unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.0 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI :R/S:U/C:N/I:L/A:L). CVE ID : CVE-2019-2807				
Improper Access Control	23-07-2019	4.4	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Gnuplot). The supported version that is affected is 11.4. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI :R/S:U/C:H/I:H/A:H). CVE ID : CVE-2019-2820	N/A		A-ORA-SO 130819/2	
	lemand_mana						
Improper Access	23-07-2019	5	Vulnerability in the Oracle Demantra Demand	N/A		A-ORA- DEMA-	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 101	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pat	ch	NCIIP	CID
Control			Manage Oracle S Suite (su Security version 7.3.1.5.2 vulneral unauthe network compro Demand Successiv vulneral unauthe subset of Demand Score 5. impacts (CVSS:3 I:N/S:U)	Supply (ubcomp). The s that is a 2. Easily bility al enticate c access mise Or l Manag ful attac bility ca of Oracle l Manag ole data. 3 (Conf). CVSS .0/AV:N /C:L/I:N	Chain Pr ponent: I supporte affected vexploit lows d attack via HT cacle Des gement. cks of th an result ead acce e Demar gement . CVSS 3 fidential Vector: N/AC:L/ N/A:N).	oducts Product ed is able er with TP to mantra is tin ess to a atra .0 Base ity PR:N/U			130819	/289
Improper Access Control	23-07-2019	4	Vulnerability in the OracleDemantra DemandManagement component ofOracle Supply Chain ProductsSuite (subcomponent: ProductSecurity). The supportedversion that is affected is7.3.1.5.2. Easily exploitablevulnerability allows lowprivileged attacker withnetwork access via HTTP tocompromise Oracle DemantraDemand Management.Successful attacks of thisvulnerability can result inunauthorized update, insert ordelete access to some of OracleDemantra Demand		N/A		A-ORA- DEMA- 130819	/290		
			vulnera unautho delete a	bility ca orized u ccess to ra Dem	an result pdate, in some o and	in nsert or f Oracle				

Weakness	Publi	sh Date	CVSS	Description & CVE ID					tch	NCIIP	CID
				(Integr Vector: (CVSS:: :N/S:U	3.0/AV:1 /C:N/I:L	ncts). CV N/AC:L/ N/A:N).	SS PR:L/UI				
				CVE ID) : CVE-2	019-27	33				
hyperion_w	ыкэр	ace		Vulner	ability ir	n the Ora	acle				
Improper Access Control	23-07	7-2019	3.5	Hyperi compo (subco Visuali versior 11.1.2. vulnera privilea networ compre Works require from a attacket this vu unauth subset Works CVSS 3 (Confic Vector (CVSS:: I:R/S:U	on Worl nent of (mponen zation). n that is 4. Easily ability al ged attac ck access omise Or pace. Succe human person of er. Succe lnerability of Oracl pace acc .0 Base S lentiality	cspace Dracle H t: UI and The sup affected exploita lows hig cker wit s via HT racle Hy ccessful interact other the ssful att ty can re ead acce e Hyper essible of Score 2.4 y impact N/AC:L/ N/A:N).	yperion l ported is able gh h TP to perion attacks tion an the acks of esult in ess to a ion lata. 4 :s). CVSS PR:H/U	N/A		A-ORA- 130819	
flexcube_inv	vestor	_servici	ng								
Improper Access Control	23-07	7-2019	5.8	Vulner FLEXC compo Service (subco Infrast	rvicing inancial	N/A	N/A		FLEX- /292		
CV Scoring So (CVSS)	cale	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	Pa	tch	NCIIF	CID
			12.0.1, 12.3.0, 14.1.0. vulnera unauth networ compre Investo attacks interac other t while t Oracle Servici signific produc this vul unauth delete a FLEXCU accessi unauth subset Investo data. C (Confic impact (CVSS:: I:R/S:C	or Servic require tion from han the a he vulne FLEXCU ng, attac cantly im cts. Succe lnerabili	12.0.4, 1 14.0.0 ar exploitab lows d attack d at	2.1.0, nd le cer with TP to EXCUBE cessful cessful con and is in stor ditional tacks of esult in nsert or of Oracle rvicing as ess to a CUBE essible ore 6.1 tegrity PR:N/U				
Improper Access Control	23-07-2019	5.5	Vulner FLEXCU compo Service (subco Infrastr versior 12.0.1, 12.3.0,	ability in UBE Inve nent of (es Applic mponen ructure) ns that an 12.0.3, 1 12.4.0, 1 Easily es	n the Ora estor Se Dracle F ations t: . Suppor re affect 12.0.4, 1	acle rvicing inancial rted ed are 2.1.0, nd	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptic	on & CVE	Pa	tch	NCIIF	CID	
			privileg networ compre- Investo attacks can res creatio modifie data or Investo data as access comple FLEXC accessi Score & Integri Vector (CVSS: :N/S:U	ability al ged attac rk access omise Or or Servic s of this v sult in ur on, deleti cation ac or Servic s well as to critica ete access UBE Invo ble data 3.1 (Confi ty impace : 3.0/AV:P /C:H/I:F	cker wit s via HT racle FL ing. Suc vulnerat nauthori on or ccess to cle FLEX ing acce unautho al data o s to all (estor Se . CVSS 3 fidential cts). CVS					
Improper Access Control	23-07-2019	5.5	FLEXC compo Service (subco Infrast version 12.0.1, 12.3.0, 14.1.0. vulnera privile netwo compre Investo attacks can res update	ability in UBE Invo nent of (es Applic mponen ructure) ns that an 12.0.3, 1 12.4.0, 1 Easily en ability al ged attac rk access omise On or Servic s of this w sult in ur e, insert of e of Orac	estor Se Dracle F cations t: . Support re affect 12.0.4, 1 14.0.0 an xploitab llows low cker wit s via HT racle FL cing. Suc vulnerat nauthori	rvicing inancial eted ed are 2.1.0, nd le w h TP to EXCUBE cessful oility zed e access	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Investor Servicing accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:N). CVE ID : CVE-2019-2843		
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Investor Servicing. CVSS 3.0 Base Score 3.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :R/S:U/C:N/I:N/A:L).	N/A	A-ORA-FLEX- 130819/295

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				106						

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pat	tch	NCIIP	CID
			CVE ID	: CVE-2	019-28	45				
Improper Access Control	23-07-2019	5	Vulner FLEXCU compo Service (subco Infrast versior 12.0.1, 12.3.0, 14.1.0. vulnera unauth networ compro Investo attacks can res read ac Oracle Servici 3.0 Bas (Confic Vector (CVSS: I:N/S:U	N/A		A-ORA-FLEX- 130819/296				
Improper Access Control	23-07-2019	3.5	FLEXC compo Service (subco Infrast versior 12.0.1, 12.3.0, 14.1.0. vulnera privile	CVE ID : CVE-2019-2846 Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to		N/A		A-ORA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

2-3	3-4	4-5
	107	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle FLEXCUBE Investor Servicing. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :R/S:U/C:H/I:N/A:N).		
			CVE ID : CVE-2019-2847		
flexcube_un	niversal_banki	ng			
Improper Access Control	23-07-2019	5.8	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1-12.0.3, 12.1.0-12.4.0 and 14.0.0-14.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products.	N/A	A-ORA-FLEX- 130819/298

ļ	CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
					108						

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pa	tch	NCIIP	C ID
			vulnera unauth delete a FLEXCU accessi unauth subset Univers data. CV (Confid impact (CVSS:: I:R/S:C	sful attac ability ca access to UBE Univ able data orized r of Oracle sal Bank VSS 3.0 F dentiality s). CVSS 3.0/AV:N C/C:L/I:L	an result opdate, in o some o versal B as well read acce e FLEXC cing acce Base Sco y and Int Vector: V/AC:L/ ./A:N).	t in nsert or of Oracle anking as ess to a CUBE essible ore 6.1 tegrity PR:N/U				
Improper Access Control	23-07-2019	5.5	FLEXCU composition Service (subcomposition Infrastriversion 12.0.1- and 14 exploit allows with net to composition FLEXCU Success vulneration fLEXCU accessi unauth delete a FLEXCU accessi unauth subset Universi data. C	ability in UBE Univ nent of C es Applic mponen ructure) ns that an 12.0.3, 1 .0.0-14.2 able vulu low priv etwork a promise UBE Univ sful attac ability ca norized u access to UBE Univ ability ca norized u access to UBE Univ ability ca ability ca borized r of Oracle sal Bank VSS 3.0 I dentiality	versal B Dracle Fi cations t: . Suppor re affect 2.1.0-12 2.0. Easil nerabilit vileged a access vi e Oracle versal B cks of th an result pdate, in o some o versal B as well read acce e FLEXC cing acce Base Sco	anking inancial rted ed are 2.4.0 ly ty ttacker a HTTP anking. is t in nsert or of Oracle anking as ess to a UBE essible ore 5.4	N/A		A-ORA- 130819	
			impact	s). CVSS	Vector:					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:N).		
			CVE ID : CVE-2019-2790		
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1-12.0.3, 12.1.0-12.4.0 and 14.0.0-14.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.0 Base Score 3.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :R/S:U/C:N/I:N/A:L).	N/A	A-ORA-FLEX- 130819/300
Improper Access	23-07-2019	5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications	N/A	A-ORA-FLEX-
Control		J	(subcomponent: Infrastructure). Supported versions that are affected are 12.0.1-12.0.3, 12.1.0-12.4.0		130819/301
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 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 14.0.0-14.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:U/C:L/I:N/A:N). CVE ID : CVE-2019-2794		
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.1.0-12.4.0 and 14.0.0- 14.2.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/U	N/A	A-ORA-FLEX- 130819/302

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				111						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:N/S:U/C:H/I:N/A:N).		
			CVE ID : CVE-2019-2839		
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1-12.0.3, 12.1.0-12.4.0 and 14.0.0-14.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :R/S:U/C:H/I:N/A:N). CVE ID : CVE-2019-2840	N/A	A-ORA-FLEX- 130819/303
Improper Access Control	23-07-2019	5.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are	N/A	A-ORA-FLEX- 130819/304
CV Scoring Se	rale		12.0.1-12.0.3, 12.1.0-12.4.0 and 14.0.0-14.2.0. Easily		
(CV Scoring Sc (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:H/I:H/A:N).		
micros_reta Improper Access Control	il-j 23-07-2019	Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Internal Operations). Supported versions that are affected are 12.1.0, 12.1.1, 12.1.2 and 13.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise MICROS Retail-J. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MICROS Retail-J accessible data as well	N/A	A-ORA-MICR- 130819/305	

(2733)				112						
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
			as unauthorized update, insert or delete access to some of MICROS Retail-J accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MICROS Retail-J. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:U/C:H/I:L/A:L).		
h anhalana 1			CVE ID : CVE-2019-2750		
berkeley_dl	0		Vulnerability in the Data Store		
Improper Access Control	23-07-2019	3.7	vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23 and 12.1.6.2.32. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Data Store. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/U I:R/S:U/C:H/I:H/A:H). CVE ID : CVE-2019-2760	N/A	A-ORA-BERK- 130819/306

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				11/						

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pat	tch	NCIIP	PC ID
Improper Access Control	23-07-2019	3.7	compo DB. Suj are affe 12.1.6. 12.1.6. 12.1.6. vulnera unauth logon t where compro Success human person Success vulnera takeov 3.0 Bas (Confic Availat Vectors (CVSS:: I:R/S:U	ability in nent of C pported ected are 1.26, 12. 1.36, 12. 2.32. Dif ability al centicate to the inf Data Sto omise Da sful attac sful attac ability ca er of Dat se Score lentiality cility imp 3.0/AV:L J/C:H/I:F	Dracle B versions e 12.1.6. 1.6.1.29 1.6.2.23 ficult to lows d attack rastruct re execu- ata Store cks requi- tion from tan the a cks of the in result a Store. 7.0 7, Integr bacts). C L/AC:H/ H/A:H).	erkeley s that 1.23, , and exploit er with ure utes to e. ire n a uttacker. is tin CVSS ity and VSS PR:N/U	N/A		A-ORA- 130819	
Improper Access Control	23-07-2019	3.7	compo DB. Suj are affe 12.1.6. 12.1.6. 12.1.6. vulnera unauth logon t where compro Success human person	ability in nent of C pported ected are 1.26, 12. 1.36, 12. 2.32. Dif ability al centicate to the inf Data Sto omise Da sful attac other th sful attac	Dracle B versions 12.1.6. 1.6.1.29 1.6.2.23 ficult to lows d attack rastruct re exect ata Store cks requision from	erkeley s that 1.23, , and exploit er with ure ites to e. ire n a uttacker.	N/A		A-ORA- 130819	
CV Scoring So	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in takeover of Data Store. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/U I:R/S:U/C:H/I:H/A:H).		
			CVE ID : CVE-2019-2869		
Improper Access Control	23-07-2019	3.7	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23 and 12.1.6.2.32. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Data Store. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/U I:R/S:U/C:H/I:H/A:H). CVE ID : CVE-2019-2870	N/A	A-ORA-BERK- 130819/309
Improper Access Control	23-07-2019	3.7	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23 and	N/A	A-ORA-BERK- 130819/310
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.1.6.2.32. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Data Store. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/U I:R/S:U/C:H/I:H/A:H).		
			CVE ID : CVE-2019-2871		
food_and_b	everage_applic	cations			
Improper Access Control	23-07-2019	4	Vulnerability in the Oracle Hospitality Simphony component of Oracle Food and Beverage Applications. The supported version that is affected is 18.2.1. Easily exploitable vulnerability allows low privileged attacker having Import/Export privilege with network access via HTTP to compromise Oracle Hospitality Simphony. While the vulnerability is in Oracle Hospitality Simphony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	N/A	A-ORA-FOOD- 130819/311
CV Scoring S	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
				117						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Hospitality Simphony accessible data. CVSS 3.0 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:C/C:H/I:N/A:N).		
			CVE ID : CVE-2019-2833		
Improper Access Control	23-07-2019	5	Vulnerability in the Oracle Hospitality Simphony component of Oracle Food and Beverage Applications. The supported version that is affected is 18.2.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Simphony accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:U/C:H/I:N/A:N). CVE ID : CVE-2019-2836	N/A	A-ORA-FOOD- 130819/312
Improper Access Control	23-07-2019	6.4	Vulnerability in the Oracle Hospitality Gift and Loyalty component of Oracle Food and Beverage Applications. Supported versions that are affected are 9.0.0 and 9.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Gift and	N/A	A-ORA-FOOD- 130819/313
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Loyalty. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Gift and Loyalty accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Gift and Loyalty accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:U/C:H/I:L/A:N).		
,			CVE ID : CVE-2019-2763		
hyperion_p	lanning		Wele eachilite in the Oreede		
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle Hyperion Planning component of Oracle Hyperion (subcomponent: Smart View). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Planning. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Planning accessible data. CVSS 3.0 Base Score 4.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U	N/A	A-ORA-HYPE- 130819/314

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				119						

Improper Access Control 23-07-2019 21 12 23 34 45 56 67 7.8 89 408	Weakness	Publish Date	CVSS	De	escriptio	n & CVE	ID	Pa	tch	NCIIP	PC ID
Improper Access Control 23-07-2019 2.1 From a person other than the attacker. Successful attacks of this vulnerability all over the attacker. Successful attacks of this vulnerability all oracle Hyperion Planning. Successful attacks of this vulnerability and result in unauthorized creation. deletion or modification accessible data. CVSS 30.0 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS.30.0 AV:N/AC:H/PR:H/U) I:R/S:U/C:N/I:H/A:N). N/A A-ORA-HYPE-130819/315 Improper Access 23-07-2019 2.1 from a person other than the attack. or creation, deletion or modification accessible data. CVSS 30.0 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS.30.0/AV:N/AC:H/PR:H/U) I:R/S:U/C:N/I:H/A:N). N/A A-ORA-HYPE-130819/315 Improper Access 23-07-2019 5 Vulnerability in the Oracle Payments or a set of the context of t				I:R/S:U/	′C:H/I:N	N/A:N).					
Improper Access Control 23-07-2019 2.1 Form a person other than the attacker. Successful attacks of this vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Planning. Successful attacks require human interaction attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Planning accessible data. CVSS 3.0 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/U ER/S:U/C:N/I:H/A:N). N/A A-ORA-HYPE- 130819/315 PaymentS Vulnerability in the Oracle Payments component of Oracle F-Business Suite (subcomponent. File Transmission). Supported Versions that are affected are 12.1.1 · 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Payments. N/A A-ORA-HYPE- 130819/315				CVE ID :	CVE-2	019-27	70				
Improper Access Control23-07-20195Vulnerability in the Oracle Payments component of Oracle E-Business Suite (subcomponent: File Transmission). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Payments.N/AA-ORA-PAYM- AORA-PAYM- 130819/316	Access	23-07-2019	2.1	Hyperio of Oracle (subcom support affected exploit w high priv network compron Planning require 1 from a p attacker this vulr unautho deletion to critica Hyperio data. CV (Integrit Vector: (CVSS:3. I:R/S:U/	n Plann e Hyper ponen is 11.1 vulnera vileged c access mise Or g. Succes human berson o c. Succes nerabili orized c al data o n Plann SS 3.0 H ty impa	ing con rion t: Secur ion that 2.4. Diff bility all attacke via HT racle Hy essful att interact other th ssful att ty can r reation, dificatio or all Or hing acco Cts). CV	nponent ity). The is ficult to lows r with TP to perion tacks tion an the acks of esult in n access racle essible ore 4.2 SS	N/A		-	
Improper Access Control 23-07-2019 5 Payments component of Oracle E-Business Suite (subcomponent: File Transmission). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Payments. N/A A-ORA-PAYM- 130819/316	payments										
	Access	23-07-2019	5	Paymen Oracle E (subcom Transmi versions 12.1.1 - 12.2.8. E vulneral unauthe network	ts comp -Busine iponen ission). that an 12.1.3 a Casily ex bility al enticate	oonent o ess Suite Suppor re affect and 12.2 xploitab lows d attack	of e ted ed are 2.3 - le cer with ΓΡ to	N/A		-	
	CV Scoring So (CVSS)	cale 0-1	1-2	-				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Desci	ription & CVE	ID	Pa	tch	NCIIP	CID
			vulnerabili unauthoriz data or com Oracle Pays data. CVSS (Confident Vector: (CVSS:3.0/ I:N/S:U/C:)	attacks of th ty can result ed access to nplete access ments access 3.0 Base Sco iality impact AV:N/AC:L/ H/I:N/A:N).					
Improper Access Control	23-07-2019	5	Payments of Oracle E-Bi (subcompo Transmissi versions the 12.1.1 - 12. 12.2.8. East vulnerabili unauthenti network ac compromis While the v Oracle Pays significanth products. S this vulner unauthoriz subset of O accessible of Score 5.8 ((impacts). O (CVSS:3.0/ I:N/S:C/C:1	ion). Suppor lat are affect .1.3 and 12.2 ily exploitab	of e ted are ed are 2.3 - le er with TP to yments. is in ks may ditional tacks of esult in ess to a ents .0 Base ity PR:N/U	N/A		A-ORA- 130819	
Improper Access Control	23-07-2019	5	Payments of	ity in the Ora component c usiness Suite onent: File	of	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3.	- 4 4-5 121	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			version 12.1.1 12.2.8. vulnera unauth networ compro While to Oracle signific product this vu unauth subset accessi Score S impact (CVSS:: I:N/S:C	cts. Succo Inerabili orized r of Oracl ble data 5.8 (Conf cs). CVSS 3.0/AV:1 C/C:L/I:1	re affect and 12.2 xploitab llows ed attack s via HT ^r racle Pay erability its, attac pact ad essful at ity can r read acco e Payme a. CVSS 3 fidential Vector: N/AC:L/ N/A:N).	ed are 2.3 - le cer with TP to yments. r is in ks may ditional tacks of esult in ess to a ents .0 Base ity PR:N/U				
Improper Access Control	23-07-2019	6.4	networ compre Succes vulnera unauth deletio to criti Payme unauth	acle of e ted are 2.3 - le cer with TP to yments. is t in n access	N/A		A-ORA- 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 122	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
siebel core	server_fram	ework	crash (complete DOS) of Oracle Payments. CVSS 3.0 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:U/C:N/I:H/A:H). CVE ID : CVE-2019-2775		
Improper Access Control	23-07-2019	5.8	Vulnerability in the Siebel Core - Server Framework component of Oracle Siebel CRM (subcomponent: Search). Supported versions that are affected are 19.0 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Core - Server Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel Core - Server Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel Core - Server Framework accessible data as well as unauthorized read access to a subset of Siebel Core - Server Framework	N/A	A-ORA-SIEB- 130819/320
			Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector:		

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				123						

Weakness	Publ	ish Date	CVSS	I	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
				I:R/S:C	/C:L/I:I	, ,	'PR:N/U '77				
hospitality_	suite	3									
Informatio n Exposure	23-0'	7-2019	4	Hospit of Orac Applica XML In version 8.9.6, 8 Easily allows with ne TCP/IF Hospit attacks can res access comple Hospit data. C (Confic Vector (CVSS: :N/S:U	ality Sui cle Hosp ations (s aterface) ns that a 3.10.2 an exploita low prive etwork a 2 to com ality Sui s of this sult in un to critic ete access ality Sui VSS 3.0 dentialit : 3.0/AV:1	subcomp re affect ad 8.11-8 ble vuln vileged a access vi promise te8. Succ vulnerat nauthori al data c ss to all (te8 acce Base Scc y impact	ponent onent: rted aed are 3.14. erability attacker a Oracle cessful oility ized or Oracle ssible ore 6.5 ts). CVSS	N/A		A-ORA- 130819	
irecruitmen	ıt										
Improper Access Control	23-07	7-2019	5	iRecru Oracle (subco Reset). that ar 12.1.3 Easily allows attacke	itment c E-Busin mponer Suppor e affecte and 12.2 exploita unauthe er with r	n the Ora compone ess Suite ted vers ed are 12 2.3 - 12.2 ble vuln enticated network mpromi	ent of e vord ions 2.1.1 - 2.8. erability d access	N/A		A-ORA- 130819	_
CV Scoring So (CVSS)	ale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Oracle iRecruitment. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle iRecruitment. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U	
I:N/S:U/C:N/I:N/A:L).	
CVE ID : CVE-2019-2809	
graalvm Vulnerability in the Oracle CuesIVM Entermine Edition	
Improper Access23-07-20194GraalVM Enterprise Edition component: GraalVM (subcomponent: GraalVM). The supported version that is affected is 19.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle AccessN/AA-ORA- 130819Improper Access23-07-20194GraalVM Enterprise Edition, ulnerability is in Oracle oracle GraalVM Enterprise Edition. While the vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS Vector: 	
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	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			CVE ID) : CVE-2	019-28	13				
Improper Access Control	23-07-2019	4	GraalV compo (subco suppor affected exploit unauth networ protoco Oracle Edition require from a attacket this vul unauth deletio to critic GraalV accessi unauth hang of crash (Oracle Edition from a attacket this vul unauth crash (Oracle Edition from a attacket this vul unauth hang of crash (Oracle Edition from a attacket this vul unauth hang of crash (Oracle Edition	ability in M Entery nent of C mponen ted vers d is 19.0 vulnera enticate ck access ols to con GraalVM a. Success e human person c er. Success lnerabili orized c n or moo cal data M Entery ble data orized a r frequen complete GraalVM a. CVSS 3 tegrity an s). CVSS 3.0/AV:N V/C:N/I:H	prise Ed Dracle G Tracle G Tracle G Tracle G Dracle G Dra	ition raalVM The is cult to lows er with ltiple se cks tion an the acks of esult in n access racle ition cause a eatable of rise Score lability	N/A		A-ORA- 130819	
siebel_core	common_co	mpone	nts							
Improper Access Control	23-07-2019	4.9	- Comn compo CRM (s Suppor affected	ability in non Com nent of C subcomp rted vers d are 19. It to expl	ponents Dracle Si onent: H sions tha .0 and p	iebel Email). at are	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 126	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publi	ish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
				privileg networ Comme Success human person Success vulners unauth data or Siebel Compo CVSS 3 (Confic Vector (CVSS:: I:R/S:U	ged attac sk access omise Si on Comp sful atta interact other th sful atta ability ca orized a comple Core - Co nents ac .0 Base S lentiality 3.0/AV:1	cks of th an result access to te acces ommon ccessible Score 4.2 y impact	h FP to re - hire n a attacker. his attacker. his critical s to all e data. 2 cs). CVSS PR:H/U				
agile_produ	ct_life	ecycle_m	anager	nent					L		
Improper Access Control	23-02	7-2019	3.6	Agile P Oracle Suite (s Files & Suppor affecte and 9.3 vulners priviles networ Succes human person Succes vulners unauth	Vulnerability in the Oracle Agile PLM component of Oracle Supply Chain Products Suite (subcomponent: Folders, Files & Attachments). Supported versions that are affected are 9.3.3, 9.3.4, 9.3.5 and 9.3.6. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all			N/A		A-ORA-, 130819	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				127						

Improper			Oracle Agile PLM accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Agile PLM. CVSS 3.0 Base Score 5.4 (Confidentiality and Availability impacts). CVSS Vector:		
Improper Access 23-0			(CVSS:3.0/AV:N/AC:H/PR:L/U I:R/S:U/C:H/I:N/A:L). CVE ID : CVE-2019-2817		
Access 23-0	es_analyti	cal_app	plications_infrastructure		
	-07-2019	5.5	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 8.0.5-8.0.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and	N/A	A-ORA-FINA- 130819/327

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				128						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:N). CVE ID : CVE-2019-2823		
application	s_manager				
Improper Access Control	23-07-2019	5.5	Vulnerability in the Oracle Applications Manager component of Oracle E- Business Suite (subcomponent: Oracle Diagnostics Interfaces). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:H/I:H/A:N).	N/A	A-ORA-APPL- 130819/328
field_servic	e				
Improper	23-07-2019	6.8	Vulnerability in the Oracle	N/A	A-ORA-FIEL-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publis	h Date	CVSS	[Descriptio	on & CVE	ID	Pat	tch	NCIIP	CID	
Access Control				Oracle (subco Suppor affecte 12.2.3 exploit allows attacke via HT Oracle attacks interac other t while t Oracle may sig additio attacks can res Oracle Base So Integri impact (CVSS:: I:R/S:C	- 12.2.8. able vul unauthe er with n TP to con Field Se tion from han the he vulne Field Se gnificant onal process of this we cult in ta Field Se	ess Suite t: Wirele sions tha .1.1 - 12 Easily nerabilit enticated network mpromi- rvice. Su e human m a pers attacker erability rvice, at cly impa- ducts. Su vulnerat keover o rvice. CV (Confide vailabili Vector: N/AC:L/ H/A:H).	e ess). at are .1.3 and ty l access accessful on and is in tacks ct ccessful oility of /SS 3.0 entiality, ty PR:N/U					
isupport	ſ		1	r				T				
Improper Access Control	23-07-	2019	5.8	iSuppo E-Busin (subco Request that ar 12.1.3 Easily of allows attacket via HT	e affecte and 12.2	onent of te t: Servic ported v d are 12 2.3 - 12.2 ble vulne enticated network	FOracle eeversions 2.1.1 - 2.8. erability l access se	N/A		A-ORA- 130819		
CV Scoring So (CVSS)	cale	0-1	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
			attacks require l interaction from other than the a while the vulner Oracle iSupport, significantly imp products. Succes this vulnerabilit unauthorized ac data or complet Oracle iSupport data as well as u update, insert or to some of Oracl accessible data. Score 8.2 (Confi Integrity impact Vector: (CVSS:3.0/AV:N I:R/S:C/C:H/I:L, CVE ID : CVE-20	n a person ttacker and rability is in , attacks may pact additional ssful attacks of ry can result in ccess to critical e access to all accessible inauthorized r delete access le iSupport CVSS 3.0 Base dentiality and ts). CVSS /AC:L/PR:N/U /A:N).				
peoplesoft	enterprise fin	proje						
Improper Access Control	23-07-2019	rise_fin_project_costingVulnerability in the PeopleSoft Enterprise FIN Project Costing component of Oracle PeopleSoft Products (subcomponent: Projects). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Project Costing. While the vulnerability is in PeopleSoft Enterprise FIN Project Costing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in					A-ORA- 130819	
CV Scoring So	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8		

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				131						

Improper Access Control23-07-20194.9Vulnerability significantly impact additional products. Successful attacks row a nuthorized update, insert or delete access to some of PeopleSoft Enterprise FIN Project Costing accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise FIN Project Costing, CVSS 3.0 Base Score 6.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:C/C:N/LL/A:L).siebel_ui_frameworkVulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). Supported versions that are affected are 19.0 and prior. Easily exploitable vulnerability allows low privileged attacker row a person other than the attacker and while the vulnerability can result in unauthorized update, insert or delete access to some of Siebel UI Framework accessible data as well as unauthorized update, insert or delete access to a subset of Siebel UIN/A	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
siebel_ui_frameworkSiebel_ui_frameworkVulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). Supported versions that are affected are 19.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel UI Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel UI Framework accessible data as well as unauthorized readN/AA-ORA-SIEB- 130819/332				delete access to some of PeopleSoft Enterprise FIN Project Costing accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise FIN Project Costing. CVSS 3.0 Base Score 6.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:C/C:N/I:L/A:L).		
Improper Access Control23-07-20194.9Vulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). Supported versions that are affected are 19.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel UI Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel UI Framework accessible data as well as unauthorized readN/AA-ORA-SIEB- 130819/332	siebel ui fr	amework		CVE ID . CVE-2019-2031		
	Access	23-07-2019	4.9	Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). Supported versions that are affected are 19.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel UI Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel UI Framework accessible data as well as unauthorized read	N/A	

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				132						

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	CID
			CVSS 3 (Confic impact (CVSS:	work acc .0 Base S dentiality s). CVSS 3.0/AV:N /C:L/I:L/	Score 5.4 y and Int Vector: N/AC:L/	l tegrity				
			CVE ID) : CVE-2	019-28	57				
identity_ma	inager									
Improper Access Control	23-07-2019	4	Identity of Orac (subco Consol that ar and 12 exploit allows with ne to com Manag this vu unauth delete Identit data. C (Integr Vector (CVSS: :N/S:U)	ability ir y Manag cle Fusio mponen e). Supp- e affecte .2.1.3.0. cable vult low priv etwork a promise er. Succe lnerabili orized u access to y Manag VSS 3.0 I rity impa : 3.0/AV:N /C:N/I:L	er comp n Middle t: Advar orted ve d are 11 Easily nerabilit rileged a ccess vi Oracle 1 essful att ty can re pdate, in o some o er access Base Sco acts). CV V/AC:L/ /A:N).	oonent eware iced rsions .1.2.3.0 Cy ttacker a HTTP identity facks of esult in nsert or f Oracle sible re 4.3 SS PR:L/UI	N/A		A-ORA- 130819	
clusterware	9									
Improper Access Control	23-07-2019	6.8	Cluster Oracle (subco Analyz suppor affecte	ability ir ware co Support mponen er (TFA) ted vers d is 12.1 oit vulne	mponer Tools t: Trace Collect ion that .0.2.0. D	t of File or). The is ifficult	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Oracle Clusterware. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Clusterware accessible data as well as unauthorized read access to a subset of Oracle Clusterware accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Clusterware. CVSS 3.0 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:U/C:L/I:L/A:L). CVE ID : CVE-2019-2860		
sun_zfs_stor	age_appliance	5.8	Vulnerability in the Sun ZFS Storage Appliance Kit (AK) component of Oracle Sun Systems Products Suite (subcomponent: HTTP data path subsystems). The supported version that is affected is 8.8.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Sun ZFS Storage Appliance Kit (AK). Successful attacks require human interaction from a person other than the attacker and while the	N/A	A-ORA-SUN 130819/335
CV Scoring Sc					

(CVSS)	0-1	12	23	54	7.5	50	0 /	7-0	0-9	5 10
CV Scoring Scale	0-1	1_2	2-3	3-1	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
			vulnerability is in Sun ZFS Storage Appliance Kit (AK), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Sun ZFS Storage Appliance Kit (AK) accessible data as well as unauthorized read access to a subset of Sun ZFS Storage Appliance Kit (AK) accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:R/S:C/C:L/I:L/A:N). CVE ID : CVE-2019-2878				
http_server							
Improper Access Control	23-07-2019	4.3	Vulnerability in the Oracle HTTP Server component of Oracle Fusion Middleware (subcomponent: OHS Config MBeans). Supported versions that are affected are 12.1.3.0.0 and 12.2.1.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle HTTP Server accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U	N/A		A-ORA-1 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 135	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				135						

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pat	tch	NCIIP	CID
			I:N/S:U	J/C:H/I:I	N/A:N).					
			CVE ID	: CVE-2	019-27	51				
mysql										
Improper Access Control	23-07-2019	4	Server MySQL Server: Suppor affected and 5.7 exploit allows with ne multipl compre Success vulnera unauth delete a MySQL CVSS 3 (Integr Vector: (CVSS: I:N/S:U	etwork a le protoc omise My sful attac ability ca lorized u access to Server a .0 Base S ity impa 3.0/AV:N J/C:N/I:I	ent of O nponen y: Privile ions tha .44 and prior. E nerabili vileged ccess vi cols to ySQL Se cks of th n result pdate, i o some c accessib Score 2.7 cts). CV V/AC:L/ L/A:N). 019-27	erver. tis tin nsert or of le data. 7 SS PR:H/U 2 30	N/A		A-ORA- 130819	-
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or				N/A		A-ORA- 130819	•
CV Scoring So	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)		12	23	136		30		70	0.5	3 10

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:L/A:L). CVE ID : CVE-2019-2731							
Improper Access Control	23-07-2019	4	Vulnera Server of MySQL : Plugga version 5.6.44 a prior ar Easily e allows h with ne multiple compro Success vulnera unautho hang or crash (o MySQL Score 4. impacts	ability in compon (subcor able Aut) s that an and prio ad 8.0.10 xploital high priv twork a e protoc omise My ful attac bility ca orized a complete Server. .9 (Avail S). CVSS 8.0/AV:N /C:N/I:1	a the My ent of O nponent h). Supp re affect r, 5.7.26 6 and pr ole vulne vileged a ccess vi cols to ySQL Se cks of th an result bility to ntly repo e DOS) o CVSS 3.0 lability Vector: V/AC:L/ N/A:H).	SQL racle racle corted ed are o and rior. erability attacker a rver. is cause a eatable of D Base PR:H/U	N/A		A-ORA- 130819	•
Improper Access Control	23-07-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Compiling). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and				N/A		A-ORA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 137	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
			Difficul vulnera privile networ protoc MySQL attacks can res read ac MySQL CVSS 3 (Confic Vector (CVSS:: I:N/S:U	-	loit lows low cker wit s via mu mpromi Success vulnerat authori a subset accessib Score 3.1 y impact N/AC:H/ N/A:N).	W h ltiple se ful oility zed of le data. L s). CVSS				
Improper Access Control	23-07-2019	3.6	Vulner Server MySQL Server Suppor affecte 5.7.26 and privile to the i MySQL compre Succes vulner succes vulner unauth hang o crash (MySQL unauth delete MySQL CVSS 3	ability in compon (subcor Security rted vers d are 5.6 and prio ior. Easil ability al ged attac infrastru Server of omise M sful attac ability ca ability ca ability ca complet Server a complet Server a corized u access to Server a .0 Base S ity and a	n the My ent of O nponent y: Privile sions that of A4 and r and 8. y exploi lows hig cker wit cture w executes ySQL Se cks of the bility to ntly report e DOS) of as well a pdate, it o some of accessib Score 5.2	SQL racle t: eges). at are prior, 0.16 table gh h logon here s to rver. is to rver. is tin cause a eatable of is nsert or of le data.	N/A		A-ORA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI :N/S:U/C:N/I:L/A:H).		
			CVE ID : CVE-2019-2739		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: XML). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2740	N/A	A-ORA-MYSQ- 130819/342
Improper Access Control	23-07-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Log). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability	N/A	A-ORA-MYSQ- 130819/343
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2741		
Improper Access Control	nproper ccess ontrol 23-07-2019 3.5 CVE ID : CVE-2019- Vulnerability in the I Server component of MySQL (subcompone Server: Security: Rol Supported versions to affected are 8.0.12 at Difficult to exploit vulnerability allows privileged attacker v network access via n protocols to compro MySQL Server. Succe attacks of this vulner can result in unauthor ability to cause a har frequently repeatabl (complete DOS) of M Server. CVSS 3.0 Bas 5.3 (Availability imp CVSS Vector: (CVSS:3.0/AV:N/AC:		vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts).	N/A	A-ORA-MYSQ- 130819/344
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Data Dictionary). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability	N/A	A-ORA-MYSQ- 130819/345
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/U :N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2746	a	
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: GIS). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacke with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2747	N/A	A-ORA-MYSQ- 130819/346
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent:	N/A	A-ORA-MYSQ- 130819/347
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIII	PC ID
			Server: Security: Privileges). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:L/A:L). CVE ID : CVE-2019-2778				
Improper Input Validation	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Components / Services). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score	N/A		A-ORA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch		NCIIF	C ID
			4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H).				
			CVE ID : CVE-2019-2780				
Improper Input Validation	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2784	N/A		A-ORA- 130819	•
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized	N/A		A-ORA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H).		
			CVE ID : CVE-2019-2785		
Improper Input Validation	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:L/A:N). CVE ID : CVE-2019-2789	N/A	A-ORA-MYSQ- 130819/351
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker	N/A	A-ORA-MYSQ- 130819/352
CV Scoring S (CVSS)	cale 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	tch	NCIIF	PC ID
			multipl compre Success vulnera unauth delete a MySQL as well access Server 3.0 Bas (Confic impact (CVSS:: I:N/S:U	etwork a le protoc omise My sful attac ability ca norized u access to Server a as unau to a subs accessib se Score 1 dentiality s). CVSS 3.0/AV:N J/C:L/I:L	cols to ySQL Se cks of th an result pdate, it so some of accessib thorized set of My le data. 3.8 y and Int Vector: V/AC:L/ L/A:N).	rver. is t in nsert or of le data d read ySQL CVSS tegrity PR:H/U				
Improper Input Validation	23-07-2019	4	Vulner Server MySQL Server: versior 8.0.16 exploit allows with ne multipl compre Succes: vulnera unauth hang of crash (MySQL Score 6 impact (CVSS: :N/S:U)	ability in compon (subcor charset is that an and prio able vulu- low priv etwork a le protoc omise M sful attac ability ca ability ca forized a r frequen complet Server. 5.5 (Avai is). CVSS	a the My ent of O nponent cs). Supp re affect r. Easily nerabilit rileged a ccess vi cols to ySQL Se cks of th an result bility to ntly repo e DOS) o CVSS 3.0 lability Vector: V/AC:L/ I/A:H).	SQL racle t: oorted ed are ty ttacker a rver. is t in cause a eatable of 0 Base PR:L/UI	N/A		A-ORA- 130819	v
Improper	23-07-2019	4	Vulner	ability in	the My	SQL	N/A		A-ORA-	MYSQ-
CV Scoring Sc (CVSS)	ale 0-1	1-2	2-3	<mark>3-4</mark> 145	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIF	PC ID
Input Validation			Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2796			130819)/354
Improper Access Control	23-07-2019	2.3	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base	N/A		A-ORA- 130819	-
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch		NCIIF	C ID
			Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:H/U I:N/S:U/C:N/I:N/A:H).				
			CVE ID : CVE-2019-2797				
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2798	N/A		A-ORA- 130819	•
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in	N/A		A-ORA- 130819	9/357
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	:h	NCII	PC ID
			unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:L/A:H). CVE ID : CVE-2019-2800				
Improper Input Validation	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2826	N/A		A-ORA- 130819	-
Improper Input Validation	23-07-2019	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are	N/A		A-ORA- 130819	-
CV Scoring So (CVSS)	cale 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	CID
			exploit allows with ne multip compre Success vulnera unauth hang o crash (MySQL Score 4 impact (CVSS:: I:N/S:U	and prio able vult high prive etwork a le protoco omise My sful attace ability ca ability ca ability ca ar frequent orized a r frequent Server. 4.9 (Avail s). CVSS 3.0/AV:N J/C:N/I:N	nerabilit vileged a ccess vi cols to ySQL Se cks of th an result bility to ntly repo e DOS) o CVSS 3.0 lability Vector: V/AC:L/ N/A:H).	rver. is cause a eatable of D Base PR:H/U				
Improper Input Validation	23-07-2019	6.8	Vulner Server MySQL Server: version 8.0.16 exploit allows with ne multip compre Succes vulnera unauth hang of crash (MySQL Score 6 impact (CVSS: :N/S:U)	ability in compon (subcom compon (subcom compon able vulue low prive etwork a le protoco omise My sful attace ability ca lorized a r frequen complete Server. 5.5 (Avail s). CVSS 3.0/AV:N /C:N/I:N	a the My ent of O nponent zer). Sup re affect r. Easily nerabilit ileged a ccess vi cols to ySQL Se cks of th an result bility to ntly repo e DOS) o CVSS 3.0 lability Vector: V/AC:L/	SQL racle racle ported ed are ty ttacker a rver. is cause a eatable of D Base PR:L/UI	N/A		A-ORA- 130819	· ·
Improper	23-07-2019	4	Vulner	ability in	the My	SQL	N/A		A-ORA-	MYSQ-
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	<mark>3-4</mark> 149	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	PC ID
Access Control			Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2879			130819	9/361
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U	N/A		A-ORA- 130819	•
CV Scoring So (CVSS)	cale 0-1	1-2	2 -3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Improper Access Control23-07-20194EN/S:U/C:N/EN/A:H). CVE ID : CVE-2019-2752Improper Access Control23-07-20194A-ORA-MYSQ- Successful attacks of this vulnerability in the MySQL Server. Successful attacks of this vulnerability impacts). CVSS Vector: (CVSS:3.0/AV:N/A:H). CVE ID : CVE-2019-2755N/AImproper Access Control23-07-20194A-ORA-MYSQ- Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/A:H). CVE ID : CVE-2019-2755N/AImproper Access Control23-07-20194Vulnerability consult in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/A:H). CVE ID : CVE-2019-275523-07-20194Vulnerability on the MySQL Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple privocosls to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or	Weakness	Publish Date	CVSS	Description & CVE ID	Pa	tch	NCIIP	PC ID
Improper Access Control23-07-20194Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U L:N/S:U/C:N/I:N/A:H).A-ORA-MYSQ- 130819/363Improper Access Control23-07-20194Vulnerability in the MySQL Server: component of Oracle MySQL (subcomponent: Server: Optimizer). Supported vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server: Successful attacks of this vulnerability can result in unauthorized ability to cause a hang orN/AImproper Access Control23-07-20194Vulnerability in the MySQL Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server: Successful attacks of this vulnerability can result in unauthorized ability to cause a hang orN/A				I:N/S:U/C:N/I:N/A:H).				
Improper Access Control23-07-20194Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score + 9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U L:N/S:U/C:N/I:N/A:H).N/AA-ORA-MYSQ- 130819/363Improper Access Control23-07-20194Vulnerability in the MySQL Server component: Server component: Server component: Server component: Server component: Server component: Server component: Server component: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple privileged attacker with network access via multiple 				CVE ID : CVE-2019-2752				
Improper Access Control23-07-20194Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang orN/AA-ORA-MYSQ- 130819/364	Access	23-07-2019	4	Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H).	N/A			•
CV Scoring Scale	Access	23-07-2019	4	Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized	N/A			•
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	-	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2757		
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:L/A:H). CVE ID : CVE-2019-2758	N/A	A-ORA-MYSQ- 130819/365
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16	N/A	A-ORA-MYSQ- 130819/366
	cale				

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pat	tch	NCIIF	CID
			vulnera privileg networ protoco MySQL attacks can res ability frequen (compl Server. 4.9 (Av CVSS V (CVSS:: I:N/S:U	ior. Easil ability al ged attac rk access ols to con Server. of this v of this v to cause ntly repe ete DOS CVSS 3.0 railability ector: 3.0/AV:N J/C:N/I:1	lows hig cker wit via mu Success vulnerat authori a hang eatable c) of MyS 0 Base S y impact N/AC:L/ N/A:H).	gh h ltiple se ful oility zed or crash QL core ts). PR:H/U				
Improper Access Control	23-07-2019	4	Vulner Server MySQL Server: versior 8.0.16 exploit allows with ne multipl compre Success vulnera unauth hang of crash (MySQL Score 4 impact (CVSS: I:N/S:U	ability in compon (subcom FTS). Su as that an and prio able vulu high prive twork a le protoc omise My sful attace ability ca	a the My ent of O nponent upporte- re affect r. Easily nerability vileged ccess vi cols to ySQL Se cks of th an result bility to ntly repo- e DOS) o CVSS 3.0 lability Vector: V/AC:L/ N/A:H).	SQL racle t: d ed are ty attacker a rver. is cause a eatable of D Base PR:H/U	N/A		A-ORA- 130819	-
Improper	23-07-2019	4	Vulner	ability in	n the My	SQL	N/A		A-ORA-	MYSQ-
CV Scoring Sc (CVSS)	ale 0-1	1-2	2-3	3-4 153	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIF	PC ID
Access Control			Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2802			130819	9/368
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U	N/A		A-ORA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:N/S:U/C:N/I:N/A:H).		
			CVE ID : CVE-2019-2803		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2805	N/A	A-ORA-MYSQ- 130819/370
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable	N/A	A-ORA-MYSQ- 130819/371
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H).		
			CVE ID : CVE-2019-2808		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2810	N/A	A-ORA-MYSQ- 130819/372
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server.	N/A	A-ORA-MYSQ- 130819/373
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCII	PC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause hang or frequently repeatabl crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2811	e			
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supporte versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacke with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause hang or frequently repeatabl crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/ :N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2812	er N/A e a e		A-ORA- 130819	v
Improper Access Control	23-07-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 a prior. Difficult to exploit vulnerability allows high			A-ORA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.2 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/U I:N/S:U/C:N/I:L/A:N). CVE ID : CVE-2019-2814		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2815	N/A	A-ORA-MYSQ- 130819/376
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit).	N/A	A-ORA-MYSQ- 130819/377
CV Scoring Sc (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pa	tch	NCIIF	PC ID
			affected 5.7.26 a and privileg network protocod MySQL attacks can ress ability frequen (comple Server update to som accessi Score 5 Availab Vectors (CVSS:: I:N/S:U	rted vers d are 5.6 and prio ior. Easil ability al ged attac of k access ols to co server. of this v to cause ntly repe ete DOS as well a , insert c e of MyS ble data 5.5 (Integ bility imp : 3.0/AV:N J/C:N/I:1	.44 and r and 8. y exploi lows hig cker with wia mul mpromi Success rulneration authori a hang eatable c of MyS as unaut or delete QL Serv . CVSS 3 grity and pacts). C	prior, 0.16 table gh h tiple se ful oility zed or erash QL horized e access er .0 Base l VSS PR:H/U				
Improper Input Validation	23-07-2019	5.1	Server MySQL Admin Suppor affected Difficul vulnera unauth networ protoco MySQL attacks interac other t Success	ability ir compon (subcor / InnoD ted vers d are 8.0 ability al ability al ability al ability al centicate k access ols to co Server. Frequire tion from han the a sful attace ability ca	ent of O nponent B Cluste sions tha .16 and loit lows d attack wia mul mpromi Success human n a pers attacker	racle racle r). t are prior. er with tiple se ful on is	N/A		A-ORA- 130819	•
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			takeover of MySQL Server. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:R/S:U/C:H/I:H/A:H). CVE ID : CVE-2019-2822		
jdk				<u> </u>	
Improper Access Control	23-07-2019	1.9	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 7u221, 8u212 and 11.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.1	N/A	A-ORA-JDK- 130819/379
CV Scoring So					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				160						

Weakness	Publish Date	CVSS	Description & CVE ID	Ра	tch	NCIIP	CID
			(Confidentiality impacts). CVS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/ I:N/S:U/C:H/I:N/A:N). CVE ID : CVE-2019-2745				
Improper Access Control	23-07-2019	2.6	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacket and while the vulnerability is in Java SE, Java SE Embedded attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be	r N/A		A-ORA-J 130819	
CV Scoring S	cale 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	Pa	tch	NCIIP	CID
			specific throug supplic 3.0 Bas (Confic Vector: (CVSS:: I:R/S:C	-	onent, e service o the AP 3.4 y impact N/AC:H/ I/A:N).	e.g., which Is. CVSS (rs). CVSS (PR:N/U				
Improper Access Control	23-07-2019	4.3	compo (subco suppor affected Difficul vulnera unauth networ protoco SE. Suc vulnera unauth partial (partial (partial (partial This vu Java de clients Java W sandbo Java SE untrus comes rely on securit also be in the s e.g., thr which s	-	Dracle Ja t: JCE). 7 ion that SE: 8u2 loit lows d attacks wia mu mpromi attacks of an result bility to f service f Java SF ity appl ats, typi applicat applicat applicat a applets load an (e.g., co e internet sandbo applicat a compo web serv data to Base Sco	ava SE The The The The The The The The The The	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pa	tch	NCIIP	CID
			Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-2842 Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE				
Improper Access Control	23-07-2019	5	(subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U			A-ORA-J 130819	/382
(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
			I:N/S:U/C:N/I:N/A:L).				
			CVE ID : CVE-2019-2762				
Improper Access Control	23-07-2019	2.6	Vulnerability in the Java SE Java SE Embedded compor of Oracle Java SE (subcomponent: Networki Supported versions that ar affected are Java SE: 7u221 8u212, 11.0.3 and 12.0.1; J SE Embedded: 8u211. Diffi to exploit vulnerability allo unauthenticated attacker w network access via multipl protocols to compromise Ja SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attack Successful attacks of this vulnerability can result in unauthorized read access to subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployment typically in clients running sandboxed Java Web Start applications or sandboxed applets (in Java SE 8), that and run untrusted code (e. code that comes from the internet) and rely on the Ja sandbox for security. This vulnerability can also be exploited by using APIs in specified Component, e.g., through a web service whi supplies data to the APIs. O 3.0 Base Score 3.1 (Confidentiality impacts). O Vector:	nent ing). re 1, ava icult ows with le ava cker. ts, Java load .g., ava the ich		A-ORA-J 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 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	(CVSS:3.0/AV:N/AC:H/PR:N/U I:R/S:U/C:L/I:N/A:N). CVE ID : CVE-2019-2766 Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks	Patch	NCIIPC ID
Improper Access Control	23-07-2019	5	compromise Java SE, Java SE	N/A	A-ORA-JDK- 130819/384

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				165						

Γ

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			I:N/S:U/C:N/I:N/A:L).				
			CVE ID : CVE-2019-2769				
Improper Access Control	23-07-2019	5.8	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity			A-ORA-J 130819	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:U/C:L/I:L/A:N). CVE ID : CVE-2019-2816		
Improper Access Control	23-07-2019	2.6	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U	N/A	A-ORA-JDK- 130819/386

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				167						

Г

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:R/S:U/C:L/I:N/A:N).		
			CVE ID : CVE-2019-2818		
Improper Access Control	23-07-2019	2.6	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:R/S:U/C:H/I:N/A:N).	N/A	A-ORA-JDK- 130819/387

CV Scoring Scale	
(CVSS)	

0-1

1-2

2-3

168

7-8

5-6

8-9

Improper Access23-07-20191.9CVE ID : CVE-2019-2821Improper (CV Scoring ScaleImproper Access23-07-20191.923-07-20192.6Vulnerability in the Java SE. (Subcomponent: Security). Supported versions that are affected are Java SE: 7u221, 8u212 and 11.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to all Java SE accessible data. Note: This vulnerability applies to Java SE 8), that Ioda and run untrusted code (e.g., code that comes from the internet) and rely on the Java SE 8), that Ioda and run untrusted code (e.g., code that comes from the internet) and rely on the Java SE score 5.1 (ControlN/AA-ORA-JRE- 130819/388Improper Access23-07-20192.6Vulnerability in the Java SE, Java SE B), that Ioda and run and so be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.1 (CONSI 3.0 Base Score 5.1 (CONSI 3.0 Base Score 5.1) (CONSI 3.0 CVSC) Vector: (CVSS:3.0/AV:L/AC:H/PR:N/U I:N/S:U/C:H/I:N/A:N). CVE ID : CVE-2019-2745N/AA-ORA-JRE- 130819/389	Weakness	Publish Date	CVSS	Description & CVE ID	Pato	h	NCIIP	CID
Improper Access Control23-07-20191.9Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 70.221, 8u212 and 11.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to all Java SE accessible data. Note: This vulnerability applies to Java SE accessible data. Note: This vulnerability applies to Java SE accessible data. Note: This vulnerability applies to Java SE 30; bat load and run untrusted code (e.g., code that comes from the internet) and rely on the Java Sandboxed Java applets (in Java SE 8); that load and run untrusted code (e.g., code that comes from the internet) and also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/U I:M/S:U/C:H/I:N/A:N). CVEI DI: CVE-2019-2745N/AA-ORA-JRE- 130819/388				CVE ID : CVE-2019-2821				
Improper Access Control23-07-20191.9 L L L L L Thir vulnerability appression the infrastructure where Java SE: 71/221, Bu212 and 11.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: Java deployments, typically in Clients running sandboxed Java Web Start applications or security. This vulnerability can also be exploited by using APIs in the specified Component. I dom exploit to Use Twice which supplies data to the APIs. CVSS 3.0 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/U E:N/S:U/C:H/I:N/A:N).N/AA-ORA-JRE- 130819/388Improper Access23-07-20192.6Vulnerability in the Java SE, ava SE Bethedded component APIs. CVSS 3.0 Base Score 5.1 (CONFIGENTAL CVSS 3.0 Base Score 5.1) (CONFIGENTAL CVSS 3.0 Base Score 5.1) (CVSS 3.0 Base Score 5.1) (CVSS 3.0 Base Score 5.1) (CVSS 3.0 Base Score 5.1) (CVSS 3.0 Base Score 5.1) (CONFIGENTAL CVSS 3.0 Base Score 5.1) (CVSS 3.0 Asse Score 5.1) (CVSS 3.0 Asse Score 5.1) (CVSS 3.0 Asse Score 5.1) (CONFIGENTAL CVSS 3.0 Asse Score 5.1) (CVSS 3.0 Asse Score 5.1) (CVSS 3.0 Asse Score 5.1) (CVSS 3.0 Asse Score 5.1) (CVSS 3.0 Asse Score 5.1) (jre	I			1		<u> </u>	
Access 23-07-2019 2.6 Java SE Embedded component N/A 130819/389	Access	23-07-2019	1.9	component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 7u221, 8u212 and 11.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/U I:N/S:U/C:H/I:N/A:N).	N/A			
CV Scoring Scale		23-07-2019	2.6	-	N/A		-	
		cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

PC ID
_

CV Scoring Scale (CVSS)

0-1

1-2

2-3

<mark>3-4</mark> 170

4-5

5-6

8-9

Weakness	Publish Date	CVSS	Description & CVE	ID	Pat	ch	NCIIP	C ID
			(CVSS:3.0/AV:N/AC:H) I:R/S:C/C:L/I:N/A:N).	/PR:N/U				
			CVE ID : CVE-2019-27	786				
Improper Access Control	23-07-2019	4.3	Vulnerability in the Jay component of Oracle Jay (subcomponent: JCE). supported version that affected is Java SE: 802 Difficult to exploit vulnerability allows unauthenticated attack network access via mu protocols to comprom SE. Successful attacks of vulnerability can result unauthorized ability to partial denial of service (partial DOS) of Java SE This vulnerability appl Java deployments, typic clients running sandbox Java Web Start application sandboxed Java applet Java SE 8), that load are untrusted code (e.g., con comes from the intern rely on the Java sandbox security. This vulnerability also be exploited by us in the specified Compo e.g., through a web ser which supplies data to APIs. CVSS 3.0 Base Sco (Availability impacts). Vector: (CVSS:3.0/AV:N/AC:H, I:N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-28	ava SE The t is 212. ker with ltiple ise Java of this t in o cause a e E. Note: lies to cally in oxed tions or s (in d run ode that et) and ox for oility can sing APIs onent, vice the ore 3.7 CVSS /PR:N/U	N/A		A-ORA-] 130819	/390
Improper Access	23-07-2019	5	Vulnerability in the Jav Java SE Embedded con		N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIF	PC ID
Control	Publish Date	cvss	of Orac (subcor Suppor affected 8u212, SE Emb exploit allows attacke via mul compro Embed of this in unau cause a service SE, Java This vu Java de clients Java V sandbo Java SE untrust comes rely on securit also be in the s e.g., thr which s APIS. C (Availa Vector: (CVSS:: I:N/S:U	le Java S mponen ted vers d are Jav 11.0.3 a bedded: able vult unauthe r with n ltiple pro omise Jav ded. Suc vulnerab ithorized a SE Emb ilnerabil ploymer running eb Start ixed Java 8), that ted code from the tase Java (partial a SE Emb ilnerabil ploymer running eb Start ixed Java (b), that ted code from the the Java y. This v exploite sough a v supplies VSS 3.0 I bility im 3.0/AV:N	E t: Utiliti ions that a SE: 7u and 12.0 8u211.1 nerabili enticated etwork otocols to va SE, Ja cessful a oility can d ability denial o DOS) of bedded. ity appl nts, typi sandbo applicat applets load an (e.g., co e interne applets load an (e.g., co e interne sandbo applets load an (AAC:L/ N/A:L).	es). at are 221, .1; Java Easily ty access to va SE attacks n result to f f Java Note: ies to cally in xed cions or s (in d run de that et) and ox for ility can ing APIs nent, vice the ore 5.3 CVSS PR:N/U		tcn	NCIIF	
			CVE ID	: CVE-2	019-27	62				
Improper Access Control	23-07-2019	2.6	Java SE of Orac	ability in Embedo le Java S mponen	ded com	ponent	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIF	PC ID
			affecter 8u212, SE Emi to expl unauth networ protoco SE, Java Success human person Success vulnera unauth subset Embed Note: T applies typical sandbo applets and run code th interne sandbo vulnera exploit specific throug supplies (Confic Vectors (CVSS:: I:R/S:U	sful attac ability ca ability ca of Java S ded acce This vuln to Java by in clie oxed Java ations or s (in Java n untrus at come et) and ro ox for sec ability ca ed by us ed Comp h a web es data to se Score lentiality 3.0/AV:N J/C:L/I:N	a SE: 7u and 12.0 8u211.1 erability d attack a via mu bedded. clos requi- clos from an result ead acce E, Java S essible d erability deployn nts runn a Web St sandbo a SE 8), t ted code s from t eay on th curity. T an also b ing APIs onent, e service b the AP 3.1 y impact V/AC:H/ V/A:N). 019-27	221, .1; Java Difficult allows er with ltiple se Java ire n a attacker. is t in ess to a SE lata. y nents, ning cart xed Java hat load e (e.g., he ne Java hat load e (e.g., he s in the Se in the Se in the Se in the Se S. CVSS (PR:N/U 66				
Improper Access	23-07-2019	5	Java SE	ability ir Embedo cle Java S	ded com		N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Control (subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, Bu212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SF, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java deployments, typically in clients running sandboxed Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:U/C:N/I:N/A:L). A-ORA-IRE- 130819/394 Improper Access Control 23-07-2019 5.8 Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are N/A A-ORA-IRE- 130819/394	Weakness	Publi	ish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
Access23-07-20195.8of Oracle Java SEN/AA-ORA-JRE- 130819/394Control $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	Control				(subcor Suppor affected 8u212, SE Emb exploit allows attacke via mul compro Embed of this via cause a service SE, Java This via Java de clients Java W sandbo Java SE untrust comes rely on securit also be in the s e.g., thr which s APIs. C (Availa Vector: (CVSS: I:N/S:U	mponent ted vers d are Jav 11.0.3 a bedded: 8 able vult unauthe r with no ltiple pro- omise Jav ded. Suc vulnerab thorized a SE Emb dinerabili ploymer running eb Start a sxed Java 8), that ted code from the the Java y. This vi exploite specified rough a v supplies VSS 3.0 H bility im 3.0/AV:N	t: Utilitions that a SE: 7u nd 12.0. Bu211. In nerabilitinticated etwork of tocols to va SE, Ja cessful a oility car d ability denial o DOS) of bedded. ity applicat applets load and (e.g., co e interne sandbo applicat applets load and (e.g., co e interne sandbo ulnerab d by usi Compot veb serv data to Base Sco pacts). (I/AC:L/ V/A:L).	es). t are 221, 1; Java Easily Easily y access o va SE attacks n result to f Java Note: les to cally in xed ions or cally in xed ions or cally in xed ions or cally in xed ions or cally in xed ions or cally in xed ions or co cally in xed ions or co cally in xed ions or co cally in xed ions or co cally in xed ions or co cally in xed ions or co cally in xed ions or co co cally in xed ions or co co co co co co co co co co				
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Access	23-07	7-2019	5.8	of Orac (subco	le Java S mponent	E t: Netwo	orking).	N/A			
(CVSS)	-	cale	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	Ра	tch	NCIIF	PC ID
			affecte 8u212, SE Emi to expl unauth netword protocc SE, Java Success vulnera delete SE, Java accessi unauth subset Embed Note: T applies typical sandbo applica and rut code th interne sandbo vulnera exploit specific throug supplie SUCCE ID	d are Jav d are Jav (11.0.3 a bedded: oit vulne enticate ck access ols to con a SE Emb sful attac ability ca access to a SE Emb ble data orized u access to a SE Emb ble data for Java S ded acce this vuln s to Java S ded acce this vuln s (in Java s (in Java)) (in Java s (in Java)) (in Java s (in Java)) (in Jav	a SE: 7u and 12.0 8u211.1 erability d attack s via mu mpromi bedded. cks of the apdate, i b some c bedded as well ead acce E, Java S essible d erability deploym nts runn a Web St sandbo SE 8), t ted code s from t ely on the curity. T an also b ing APIs onent, e service b the AP 4.8 7 and In Vector: V/AC:H/ 2/A:N). 019-28	221, .1; Java Difficult allows er with ltiple se Java is t in nsert or of Java as ess to a SE lata. y nents, ning tart xed Java hat load e (e.g., he ne Java hat load e (e.g., he s in the s in the s in the s in the s in the s fara hat load e (e.g., he ne Java hat load e (e.g., he las CVSS tegrity				
Improper Access	23-07-2019	2.6	compo	ability in nent of (mponen)racle Ja	iva SE	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 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	C	Descriptio	n & CVE	ID	Pa	tch	NCIIF	PC ID
Weakness Control	Publish	n Date	CVSS	Suppor affected 12.0.1. vulnera unauth networ protoco SE. Suc human person Success vulnera unauth subset data. N applies typicall sandbo applica applets and run code th interne sandbo vulnera Java de servers trusted installe CVSS 3 (Confid Vector: (CVSS:3	ted vers d are Jav Difficult ability al enticate k access ols to con cessful a interact other th sful attac ability ca orized r of Java S ote: This to Java S ote: This to Java G ly in clies at Java G ly in clies at ons or s (in Java at come et) and re ox for sec ability do ploymer s, that loa code (en solution of sec ability do ploymer s, that loa	ions tha a SE: 11 to explo lows d attack via mu mpromi attacks r ion from an the a cks of the ead acce E access s vulners deployn nts runn a Web St sandbo SE 8), t ted code s from t ely on th curity. T oes not a nts, typic ad and r g., code adminis Score 3.1 y impact	at are 0.3 and oit er with ltiple se Java equire n a attacker. is t in ess to a sible ability nents, ning cart xed Java hat load e (e.g., he ne Java hat load e (e.g., he no Java hat so cally in run only	Pa	tch	NCIIF	PCID
				CVE ID	: CVE-2	019-28	18				
Improper Access Control	23-07-	2019	2.6	compor (subcor Suppor affected	ability in nent of C mponent ted vers d are Jav Difficult)racle Ja t: JSSE). ions tha a SE: 11	iva SE it are 0.3 and	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale	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	[Descriptio	on & CVE	ID	Patch		NCIIP	CID
				unauth networ compre Success human person Success vulnera unauth data or Java SE This vu Java de clients Java W sandbo Java SE untrus comes rely on securit does no deploy servers trusted installe CVSS 3 (Confic Vector (CVSS::	rk access omise Ja sful atta interact other th sful atta ability ca comple comple comple caccessi ilnerabil ployme running eb Start oxed Java 2 8), that ted code from the Java 5 8), that ted code from the a code from the s, that lo code (e ed by an .0 Base S lentiality : 3.0/AV:1	ed attack s via TLS va SE. cks requi- tion from nan the a cks of th an result access to te access ble data. lity appli- nts, typi- g sandbo applicat a applets cload an e (e.g., co e interne a sandbo rulnerab to Java ypically ad and r e.g., code adminis Score 5.3 y impact	S to iire n a attacker. is t in critical s to all . Note: ies to cally in xed cions or s (in d run ode that et) and ox for ility in run only strator). 3 cs). CVSS /PR:N/U				
outside_in_t	techno	ology							I		
Improper Access Control	23-07	7-2019	7.5	Outside compo Middle Outside	e In Tech nent of (ware (se e In Filte	n the Ora hnology Oracle Fr ubcomp ers). The sion that	usion onent:	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	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	[Descriptio	n & CVE	ID	Ра	tch	NCIIF	PC ID
Weakness	Publish Date	CVSS	affected exploit allows attacke via HT Oracle Success vulnera unauth delete a Outside accessi unauth subset Techno and un cause a service Outside Suite of kits (SI CVSS so softwa In Tech score a softwa over a Outside but if d a netwo be lowo 7.3 (Co and Av	d is 8.5.4 able vult unauthe er with n TP to con Outside sful attac ability ca ability ca access to e In Tech ble data orized r of Oracle ology acc authoriz authoriz e (partial e In Tech f softwar OKs). The core dep re that u nology of ssumes re passes network e In Tech data is no ork the C er. CVSS onfidentia	k. Easily nerabilit enticated etwork mpromis In Techs cks of the pdate, in o some o nology as well ead acce e Outsid cessible ced abilit denial o DOS) of nology. nology ce develo e protoc end on t ses the code. The that the s data re- cidirectly nology treceiv CVSS sco 3.0 Base ality, Inter V/AC:L/ L/A:L).	ty access se nology. is in nsert or of Oracle as ess to a e In data ty to f f Oracle Note: is a opment col and the Outside e CVSS eceived y to code, ed over ore may e Score tegrity (s). CVSS		tch	NCIIF	
Improper Access	23-07-2019	7.5	Vulner Outside compo		N/A		A-ORA- 130819			
CV Scoring So (CVSS)	cale 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	on & CVE	ID	Ра	tch	NCIIP	CID
Control			Middle	ware (si	ubcomp	onent:				
			Outsid	e In Filte	ers). The	2				
			suppor	ted vers	ion that	is				
			affecte	d is 8.5.4	ł. Easily					
			_	able vul						
			allows	unauthe	enticated	ł				
			attacke	er with n	etwork	access				
			via HT'	TP to co	mpromi	se				
				Outside						
			Succes	sful atta	cks of th	is				
				ability ca						
			unauth	orized u	ipdate, i	nsert or				
			delete	access to	o some c	of Oracle				
				e In Tecl	05					
			accessi	ble data	as well	as				
			unauth	orized r	ead acce	ess to a				
			subset	of Oracl	e Outsid	le In				
			Techno	ology acc	cessible	data				
			and un	authoriz	zed abili	ty to				
			cause a	o partial	denial o	f				
			service	(partial	DOS) o	f Oracle				
			Outsid	e In Tecl	nnology.					
			Outsid	e In Tecl	nnology					
			suite o	f softwa	re devel					
			kits (Sl	OKs). Th	e protoc	col and				
			CVSS s	core dep	end on	the				
			softwa	re that u	ises the	Outside				
			In Tecł	nnology	code. Th	e CVSS				
			score a	ssumes	that the					
			softwa	re passe	s data re	eceived				
			over a	network	directly	y to				
			Outsid	e In Tecl	nnology	code,				
			but if d	lata is no	ot receiv	ed over				
			a netw	ork the (CVSS sco	ore may				
			be low	er. CVSS	3.0 Bas	e Score				
			7.3 (Co	nfidenti	ality, Int	tegrity				
			and Av	ailability	y impact	s). CVSS				
			Vector	:						
			(CVSS:	3.0/AV:I	N/AC:L/	PR:N/U				
			I:N/S:U	J/C:L/I:I	L/A:L).					
				: CVE-2						
CV Scoring S	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)				179						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	23-07-2019	7.5	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	N/A	A-ORA-OUTS- 130819/399
CV Scoring S					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
180										

Access Control 23-07-2019 7.5 unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score	Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pa	tch	NCIIP	C ID
Improper Access Control 23-07-2019 7.5 Vulnerability in the Oracle Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score				-	-	• •	PR:N/U				
Improper Access Control23-07-20197.5Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to assubset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology so success ful atenda of service (partial DOS) of Oracle Outside In Technology or of software that uses the Outside In Technology code, The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base ScoreN/AA-ORA-OUTS- 130819/400				,		, ,					
Improper Access Control23-07-20197.5Outside In Technology component of Oracle Qutside In Technology. Successful attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to a subset of Oracle Outside In Technology accessible data as unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. N/AA-ORA-OUTS- 130819/400Control7.5unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code, but if data is not received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base ScoreN/A											
CV Scoring Scale	Improper Access Control		7.5	Outside compo Middle Outside suppor affected exploit allows attacke via HT Oracle Success vulnera unauth delete a Outside accessi unauth subset Techno and un cause a service Outside Suite of kits (SI CVSS so softwa In Tech score a softwa over a Outside a netwo	e In Tech nent of C ware (su e In Filte ted vers d is 8.5.4 able vult unauthe er with n TP to con Outside sful attac ability ca orized u access to e In Tech ble data orized r of Oracle ology acc authoriz partial e In Tech f softwar DKs). The core dep re that u unology of sumes re passes network e In Tech ata is no ork the C	inology Dracle F abcompo- ion that ion that ion that is. Easily nerabili- nticated etwork mpromi In Tech cks of the pdate, i pdate, i pdate, i o some c anology as well ead acce e Outsid cessible ied abili denial o DOS) of mology re devel- e protoc end on ses the code. The that the s data re directly mology t receiv CVSS sco	usion onent: is is ty l access se nology. is t in nsert or of Oracle as ess to a le In data ty to f f Oracle is a opment col and the Outside ae CVSS eceived y to code, ed over ore may	N/A			
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	-	CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6					5-6	6-7	7-8	8-9	9-10

Improper Access Control 23-07-2019 7.5	Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
Improper Access Control23-07-20197.5Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The 				and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U				
Improper Access Control23-07-20197.57.5Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is 				CVE ID : CVE-2019-2759				
over a network directly to Outside In Technology code,	Access	23-07-2019	7.5	Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to	N/A			
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1		cale 0-1	1-2	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
			but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:U/C:L/I:L/A:L). CVE ID : CVE-2019-2764				
Improper Access Control	23-07-2019	7.5	CVE ID : CVE-2019-2764Vulnerability in the OracleOutside In Technologycomponent of Oracle FusionMiddleware (subcomponent:Outside In Filters). Thesupported version that isaffected is 8.5.4. Easilyexploitable vulnerabilityallows unauthenticatedattacker with network accessvia HTTP to compromiseOracle Outside In Technology.Successful attacks of thisvulnerability can result inunauthorized update, insert ordelete access to some of OracleOutside In Technologyaccessible data as well asunauthorized read access to asubset of Oracle Outside InTechnology accessible dataand unauthorized ability tocause a partial denial ofservice (partial DOS) of OracleOutside In Technology. Note:Outside In Technology is asuite of software developmentkits (SDKs). The protocol andCVSS score depend on thesoftware that uses the OutsideIn Technology code. The CVSSscore assumes that the	N/A		A-ORA- 130819	
CV Scoring S (CVSS)	cale 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	Pa	tch	NCIIP	C ID
			over a Outsid but if d a netw be low 7.3 (Co and Av Vector (CVSS:: I:N/S:U	-	t directly mology of receiv CVSS sco 3.0 Base ality, Inf / impact V/AC:L/ L/A:L).	y to code, ed over ore may e Score cegrity cs). CVSS PR:N/U				
Improper Access Control	23-07-2019	7.5	Vulner Outside compo Middle Outside suppor affecte exploit allows attacke via HT Oracle Success vulner unauth delete Outside accessi unauth subset Techno and un cause a service Outside Suite o kits (SI	ability in e In Tech nent of (ware (su e In Filte ted vers d is 8.5.4 cable vult unauthe er with n TP to con Outside sful attac ability ca	n the Ora nology Dracle F abcomp- ers). The ion that Easily nerability enticated etwork mpromi In Tech cks of th an result pdate, i o some c nology as well ead acce e Outsid cessible denial o DOS) of nology re develo	acle usion onent: is ty l access se nology. is t in nsert or of Oracle as ess to a e In data ty to f f Oracle kits is a opment col and	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Improper Access Control 23-07-2019 7.5 S Valuerability and value in Technology. Successible data as well as unauthorized update, insert or delete access to a subset of Oracle Outside In Technology. N/A A-ORA-OUTS- 130819/404 Improper Access Control 23-07-2019 7.5 S S 3.4 4.5 5.6 6.7 7.8 8.9 9.01	Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
Improper Access Control 23-07-2019 7.5				In Tech score a softwa over a Outsid but if d a netw be low 7.3 (Co and Av Vector (CVSS: I:N/S:U	nnology issumes re passe network e In Tecl lata is no ork the 0 er. CVSS onfidenti railability : 3.0/AV:1 J/C:L/I:1	code. Th that the s data re directly nology ot receiv CVSS sco 3.0 Base ality, Int y impact N/AC:L/ L/A:L).	e CVSS eceived 7 to code, ed over ore may e Score cegrity ts). CVSS PR:N/U				
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Access	23-07-2019	7.5	Vulner Outsid compo Middle Outsid suppor affecte exploit allows attacke via HT Oracle Succes vulner unauth delete Outsid accessi unauth subset Techno and un cause a service Outsid	n the Ora nology Dracle Fi abcompo- ers). The sion that Easily nerability enticated etwork in Techi cks of the pdate, in pdate, in pdate, in po some of nology as well ead acce e Outsid cessible of zed ability denial of DOS) of nology.	acle usion onent: is ty l access se nology. is tin nsert or of Oracle as ess to a e In data ty to f f Oracle Note:	N/A				
	-	cale 0-1	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ſ	Descriptio	on & CVE	ID	Pa	tch	NCIIP	PC ID
			kits (SI CVSS s softwa In Tech score a softwa over a Outside but if d a netw be low 7.3 (Co and Av Vector (CVSS:: I:N/S:U	:	e protoc eend on ses the code. Th that the s data re directly nology of receiv CVSS scc 3.0 Bas ality, Int y impact N/AC:L/ L/A:L).	col and the Outside the CVSS eceived y to code, ed over ore may e Score tegrity cs). CVSS PR:N/U				
Improper Access Control	23-07-2019	7.5	Vulner Outside compo Middle Outside suppor affecte exploit allows attacke via HT Oracle Succes vulner unauth delete Outside accessi unauth subset Techno and un	n the Ora nnology Dracle F ubcomp ers). The sion that t. Easily nerabili enticated etwork mpromi In Tech cks of the an result	acle usion onent: is is ty access se nology. is t in nsert or of Oracle as ess to a le In data ty to	N/A		A-ORA- 130819		
CV Scoring So (CVSS)	cale 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	tch	NCIIF	PC ID
			Outside Suite of kits (SI CVSS se softwa In Tech score a softwa over a Outside but if d a netwo be lowo 7.3 (Co and Av Vectors (CVSS:: I:N/S:U	e In Tech e In Tech f softwa DKs). Th core dep re that u nology assumes re passe network e In Tech lata is no ork the er. CVSS onfidenti railability : 3.0/AV:1	e protoc bend on uses the code. Th that the es data re directly hnology bt receiv CVSS sco 3.0 Bas dality, Int y impact N/AC:L/ L/A:L).	Note: is a opment col and the Outside he CVSS eceived y to code, ed over ore may e Score tegrity cs). CVSS				
vm_virtualb	OX				1017 20					
Improper Access Control	23-07-2019	2.1	Virtual Oracle (subco Suppor affected prior to exploit allows with lo infrast VM Vir compre Virtual vulnera Virtual signific	TE ID : CVE-2019-2855 Inerability in the Oracle VM tualBox component of acle Virtualization bcomponent: Core). pported versions that are ected are Prior to 5.2.32 and for to 6.0.10. Easily ploitable vulnerability ows low privileged attacker th logon to the trastructure where Oracle I VirtualBox executes to mpromise Oracle VM tualBox. While the Inerability is in Oracle VM tualBox, attacks may mificantly impact additional oducts. Successful attacks of		N/A		A-ORA- 130819	-	
CV Scoring So	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS)				107	+ 3	2.0		, 0		5.10
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 & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI :N/S:C/C:N/I:N/A:H). CVE ID : CVE-2019-2848		
Improper Access Control	23-07-2019	1.9	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 2.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI :R/S:U/C:N/I:N/A:L).	N/A	A-ORA-VM_V- 130819/407
Improper Access Control	23-07-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization	N/A	A-ORA-VM_V- 130819/408
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 188	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	PC ID
			Suppor affected prior to exploit allows with lo infrastr VM Vir compro Virtual vulnera Virtual signific produc this vul takeove Virtual Score 8 Integrif impact (CVSS: :N/S:C/	mponent rted vers d are Pri o 6.0.10. rable vult low priv gon to th ructure v tualBox omise Or Box. Wh ability is Box, atta cantly im cts. Succe lnerabili er of Ora Box. CVS 3.8 (Conf ty and Av s). CVSS 3.0/AV:L /C:H/I:H	sions tha or to 5.2 Easily nerabilit rileged a ne where O executes racle VM ile the in Oracl acks may pact add essful att ty can re acle VM SS 3.0 Ba identiali vailabili Vector: 2/AC:L/I	at are 2.32 and ty ttacker racle s to I le VM ditional tacks of esult in ase ity, ty PR:L/UI				
Improper Access Control	23-07-2019	2.1	Virtual Oracle (subcon Suppor affected prior to exploit allows with lo infrastr VM Virt compro Virtual vulnera	ability in Box com Virtualiz mponent rted vers d are Pri o 6.0.10. rable vulu low priv gon to th ructure v tualBox omise Or Box. Wh ability is Box, atta	aponent zation t: Core). sions tha or to 5.2 Easily nerabilit rileged a ne where O executes racle VM ile the in Oracl	of at are 2.32 and ty ttacker racle s to I le VM	N/A		A-ORA- 130819	
				antly im						

Weakness	Publish Date	CVSS	Descript	ion & CVE	ID	Pa	tch	NCIIF	PC ID
			products. Suc this vulnerabi unauthorized data or compl Oracle VM Vir accessible dat Score 6.5 (Con impacts). CVS (CVSS:3.0/AV :N/S:C/C:H/I: CVE ID : CVE-	ility can r access to lete acces tualBox a. CVSS 3 nfidential S Vector: :L/AC:L/ N/A:N).	esult in critical s to all .0 Base ity PR:L/UI				
Improper Access Control	23-07-2019	4.4	Vulnerability VirtualBox co Oracle Virtual (subcompone Supported ver affected are P prior to 6.0.10 exploit vulner high privilege logon to the in where Oracle executes to co Oracle VM Vir the vulnerabil VM VirtualBox significantly in products. Such this vulnerabil takeover of Or VirtualBox. CV Score 7.5 (Con Integrity and impacts). CVS (CVSS:3.0/AV I:N/S:C/C:H/I	in the Ora mponent lization ent: Core). rsions tha rior to 5.2 D. Difficul rability all ed attacke ofrastruct VM Virtu ompromise tualBox. T lity is in C x, attacks mpact ad cessful at ility can r racle VM VSS 3.0 Ba nfidential Availabili S Vector: EL/AC:H/	acle VM of at are 2.32 and t to lows r with cure alBox se While Dracle may ditional tacks of esult in ase ity, ty PR:H/U	N/A		A-ORA- 130819	_
Improper Access Control	23-07-2019	4.4	Vulnerability VirtualBox co Oracle Virtual	mponent		N/A		A-ORA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			Suppor affected prior to exploit high pr logon t where execute Oracle the vul VM Vir signific produc this vul takeove Virtual Score 7 Integrif impact (CVSS:3 I:N/S:C		sions tha or to 5.2 Difficult bility all attackes rastruct M Virtus npromis ualBox. V ty is in O attacks upact add essful att ty can re acle VM SS 3.0 Ba fidentiali vailabili Vector: L/AC:H/ H/A:H).	at are 2.32 and t to lows r with aure alBox se While Dracle may ditional tacks of esult in ase ity, ty PR:H/U				
Improper Access Control	23-07-2019	4.6	I:N/S:C/C:H/I:H/A:H). CVE ID : CVE-2019-2865 Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional		N/A		A-ORA- 130819	_		
	1		products. Successful attacks of2-33-44-55-6							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI :N/S:C/C:H/I:H/A:H).		
			CVE ID : CVE-2019-2866		
Improper Access Control	23-07-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI :N/S:C/C:H/I:H/A:H). CVE ID : CVE-2019-2867	N/A	A-ORA-VM_V- 130819/413
Improper Access Control	23-07-2019	2.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core).	N/A	A-ORA-VM_V- 130819/414
CV Scoring So	cale 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	tch	NCIIF	CID
			affecte prior to exploit allows with lo infrast: VM Vir compre Virtual of this in unau cause a service VM Vir Score 3 impact (CVSS: :N/S:U	rted vers d are Pri o 6.0.10. able vul low priv gon to the ructure tualBox omise Or Box. Suc vulneral athorize partial tualBox. 3.3 (Avai s). CVSS 3.0/AV:I /C:N/I:N	ior to 5.2 Easily nerabili vileged a he where 0 execute racle VM ccessful oility can d ability denial o DOS) o CVSS 3 lability Vector: L/AC:L/					
				: CVE-2						
Improper Access Control	23-07-2019	2.1	Virtual Oracle (subco Suppor affecte prior to exploit allows with lo infrast VM Vir compre Virtual of this in unau cause a	at are 2.32 and 2.32 and ty attacker racle s to I attacks n result to f f Oracle 0 Base	N/A		A-ORA- 130819	-		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:L/AC:L/PR:L/UI :N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-2874		
Improper Access Control	23-07-2019	2.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI :N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-2875	N/A	A-ORA-VM_V- 130819/416
Improper Access Control	23-07-2019	2.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM	N/A	A-ORA-VM_V- 130819/417
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	PC ID
			of this v in unau cause a service VM Virt Score 3 impacts (CVSS:3 :N/S:U/	Box. Suc vulnerab ithorized partial (partial tualBox. 3.3 (Avail s). CVSS 3.0/AV:L /C:N/I:N	bility car d ability denial o DOS) of CVSS 3. lability Vector: L/AC:L/I	n result to f f Oracle 0 Base PR:L/UI				
Improper Access Control	23-07-2019	2.1	Vulnera Virtual Oracle (subcon Suppor affected prior to exploit allows with log infrastr VM Virt compro Virtual of this v in unau cause a repeata DOS) of CVSS 3. (Availa Vector: (CVSS:3 :N/S:U)	ability in Box com Virtualiz mponent rted vers d are Pri o 6.0.10. able vuln low priv gon to th ructure v tualBox or Box. Suc vulnerat able cras f Oracle .0 Base S bility im	n the Ora apponent zation t: Core). sions tha or to 5.2 Easily nerabilit rileged a ne where O executes cacle VM ccessful a bility car d ability frequents ch (comp VM Virt Score 5.5 pacts). O L/AC:L/I I/A:H).	acle VM of at are 2.32 and 2.32 and 2.32 and 2.32 and 2.32 attacker racle s to attacks a result to attacks a result to atty blete ualBox. 5 CVSS PR:L/UI	N/A		A-ORA- 130819	_
database_se	erver									
Improper Access	23-07-2019	4.9	Vulnerability in the Java VM component of Oracle Database Server. Supported versions				N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	۵	Descriptio	n & CVE	ID	Pat	tch	NCIIP	PC ID
Control			Difficul vulnera privileg Create Proced networ protoco VM. Suc vulnera unauth deletio to critic accessi unauth hang or crash (e VM. CV (Integr impact (CVSS:3 I:N/S:U	12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java VM. CVSS 3.0 Base Score 6.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/U I:N/S:U/C:N/I:H/A:H). CVE ID : CVE-2019-2749 Vulnerability in the Core						
N/A	23-07-2019	5.5	RDBMS Databa version 12.1.0.2 Easily e allows having privileg via Ora Core RI vulnera RDBMS signific produc	S components of the serve of th	nent of (er. Suppo re affect .1, 18c a ole vulne vileged a Any Inde network o compr Vhile the in Core s may upact ado essful att	Oracle orted and are and 19c. erability attacker ex access comise e ditional tacks of	N/A		A-ORA- 130819	
			unauth	orized a	ccess to	critical				

Weakness	Publish D	ate	CVSS	D	escriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
				Core RI well as insert c of Core data. CV (Confid impacts (CVSS:3 I:N/S:C	DBMS ac unautho or delete RDBMS VSS 3.0 I lentiality s). CVSS 3.0/AV:N /C:H/I:I	orized u access accessi Base Sco y and Int Vector: N/AC:L/	e data as pdate, to some ble re 7.6 tegrity PR:H/U				
Improper Access Control	23-07-20)19	6	Vulnera ODBC I Oracle 1 class=fe ***PRIV NONE I ATTAC Suppor affected 12.2.0.1 exploit low pri None p access v to comp Driver. this vul takeove Driver. affects 1 only. CV (Confid Availab Vector: (CVSS:3 I:N/S:U	ability in Driver co Databas ont-red /ILEGE (FOR AUT KS*** <br ted vers d are 11 1 and 18 vulnera vileged rivilege via mult promise Success nerabili er of Ora Note: T Window VSS 3.0 1 lentiality ility imp 3.0/AV:1 //C:H/I:1 : CVE-2	n the Ora omponent e Server > CANNOT THENTIO b>sions that .2.0.4, 12 oc. Diffict bility all attacker with net iple proo Oracle O ful attack ful a	acle nt of . at are 2.1.0.2, ult to lows having twork tocols DBC eks of esult in C erability rms ore 7.5 ity and VSS PR:L/U</span 	N/A		A-ORA- 130819	/421
N/A	23-07-20)19	4.9	Vulnerability in the Application Express		N/A		A-ORA- 130819			
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	PC ID
			Server. that are 18.2. E vulnera privileg Valid A networ compre Expres require from a attacke vulnera Expres signific produc this vul unauth delete a Applica data as read ac Applica tata. C (Confic impact (CVSS:: :R/S:C/	nent of C Support e affected asily exp ability al ged attac account p ck access omise Ap s. Success e human person c er and wl ability is s, attack cantly im cts. Succes lnerabili orized u access to ation Exp well as cess to a ation Exp VSS 3.0 F lentiality s). CVSS 3.0/AV:N /C:L/I:L/	ted vers d are 5.2 oloitable lows low cker hav orivilege s via HT oplication sful atta interact other that hile the in Appl s may opact add essful at ty can re opact add press acc asubset opaces acc asu	ions l and w ing e with TP to on acks tion an the ication ditional tacks of esult in nsert or of cessible orized of cessible ore 5.4 tegrity PR:L/UI				
Improper Access Control	23-07-2019	1.2	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Difficult to exploit vulnerability allows high privileged attacker having Local Logon privilege with logon to the infrastructure where Core RDBMS executes				N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	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	NCII	PC ID
			to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Core RDBMS accessible data. CVSS 3.0 Base Score 4.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/U I:R/S:U/C:H/I:N/A:N). CVE ID : CVE-2019-2569				
Improper Access Control	23-07-2019	4.9	Vulnerability in the Oracle Text component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via OracleNet to compromise Oracle Text. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Text accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Text. CVSS 3.0 Base Score 4.6 (Confidentiality and Availability impacts). CVSS			A-ORA- 130819	
CV Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:L/UI :R/S:U/C:L/I:N/A:L). CVE ID : CVE-2019-2753		
application	_testing_suite				
Improper Access Control	23-07-2019	7.5	Vulnerability in the Oracle Application Testing Suite component of Oracle Enterprise Manager Products Suite (subcomponent: Load Testing for Web Apps). The supported version that is affected is 13.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data as well as unauthorized read access to a subset of Oracle Application Testing Suite accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Testing Suite. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:U/C:L/I:L/A:L). CVEID: CVE-2019-2727	N/A	A-ORA-APPL- 130819/425
business_in	telligence_pub	lisher		I	
Improper	23-07-2019	6.4	Vulnerability in the Oracle BI	N/A	A-ORA-BUSI-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 200	6-7	7-8 8-9 9-10

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	ID	Pa	tch	NCIIP	PC ID
Access Control			API). T that is Easily allows attacke via HT Oracle vulner Publish signific produc this vu unauth delete BI Pub well as access Publish CVSS 3 (Confic impact (CVSS: I:N/S:C	(subcomponent: Web Service API). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. While the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.0 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:N/S:C/C:L/I:L/A:N). CVE ID : CVE-2019-2742					130819	9/426
one-to-one_	fulfillment									
Improper Access Control	23-07-2019	5.8	One-to compo Busine (subco Suppor affecte 12.2.3 exploit allows attacke	ability in -One Fui nent of G ss Suite mponen rted vers d are 12 - 12.2.8. rable vul unauthe er with m TP to co	lfillment Dracle E- sions tha .1.1 - 12 Easily nerabilit enticated	Server). It are .1.3 and Ly I access	N/A		A-ORA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 201	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIF	PC ID
			Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:R/S:C/C:H/I:L/A:N).				
Improper Access Control	23-07-2019	5.8	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E- Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptic	on & CVE	ID	Pa	tch	NCIIP	CID
			signific product this vu unauth data or Oracle accessi unauth delete One-to accessi Score & Integri Vector (CVSS:: I:R/S:C	acks ma pact ad essful at ity can r access to te acces One Fulf as well pdate, i o some c fillment . CVSS 3 fidential cts). CVS	ditional ditional tacks of esult in critical s to all fillment as nsert or of Oracle .0 Base ity and S PR:N/U					
Improper Access Control	23-07-2019	5.8	I:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2019-2668 Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E- Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of				N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Pat	tch	NCIIP	PC ID
			unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2019-2672							
			CVE ID	: CVE-2	019-26	72				
application_o	object_library	7								
Improper Access Control	23-07-2019	4.3	Applica compo Busine (subco / File U version 12.1.3 a Difficul vulnera unauth networ compro Applica Success vulnera unauth subset Object CVSS 3 (Confic Vector: (CVSS:3	.0 Base S lentiality	ject Libr Dracle E t: Attach Support re affect 2.3 - 12.2 loit lows d attack s via HT cacle ject Libr cks of th an result ead acce e Applic accessib Score 3.7 y impact N/AC:H/ N/A:N).	rary ments ed ed are 2.8. rer with TP to rary. is t in ess to a ation ble data. 7 ts). CVSS PR:N/U	N/A		A-ORA- 130819	
1										

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	h	NCIIPC ID
crm_technic	cal_foundation					
Improper Access Control	23-07-2019	5.8	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E- Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:R/S:C/C:H/I:L/A:N).	N/A		A-ORA-CRM 130819/431
weblogic_se	erver 23-07-2019	5.5	Vulnorability in the Oracle	N/A		A-ORA-WEBL
Improper CV Scoring So	cale		Vulnerability in the Oracle		7.0	
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-6 205	6-7	7-8	8-9 9-10

Access ControlWebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to all Oracle WebLogic Server accessible data or complete access to all Oracle WebLogic Server accessible data or complete accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U) L:N/S:U/C:H/:L/A:N).N/AA-ORA-WEBL- 130819/433Improper Access Control23-07-20195.55.5Vulnerability allows high privileged attacker with network access via HTTP to components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability a	Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Pa	tch	NCIIP	PC ID
Improper Access Control23-07-20195.5WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result inN/AA-ORA-WEBL- 130819/433				of Orac (subcon Compo version 10.3.6.0 12.2.1.3 vulnera privileg networ compro Server. this vul unauth data or Oracle accessi unauth delete a WebLo data. CV (Confid impact (CVSS:3 I:N/S:U	ele Fusio mponen nents). S as that an 0.0, 12.1 3.0. Easi ability al ged attac brized attac comise On Success lnerabili orized a comple WebLog ble data orized u access to gic Serv VSS 3.0 I lentiality s). CVSS 3.0/AV:P	n Middle t: WLS (Support re affect .3.0.0 ar ly explo- lows hig cker wit s via HT racle We ful attac ity can re access to te acces gic Serve as well update, it o some o er acces Base Sco y and Int Vector: N/AC:L/ L/A:N).	eware Core ed ed are ad itable gh h CP to ebLogic ebLogic eks of esult in critical s to all r as nsert or of Oracle sible ore 5.5 tegrity PR:H/U			130819	9/432
unauthorized access to critical	Access	23-07-2019	5.5	WebLo of Orac (subcon Compo version 10.3.6.0 12.2.1.3 vulnera privileg networ compro Server. this vul	gic Serv ele Fusio mponen nents). S as that an 0.0, 12.1 3.0. Easi ability al ged attac what access omise On Success Inerabili	er comp n Middle t: WLS (Supporte re affect .3.0.0 ar ly explo llows hig cker wit s via HT racle We ful attac	onent eware Core ed ed are id itable gh h FP to ebLogic eks of esult in	N/A			
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	-	cale <u>0</u> -1	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			delete a WebLog data. CV (Confid impacts	WebLog ole data orized u ccess to gic Serve /SS 3.0 F entiality S). CVSS S.0/AV:N /C:H/I:I	ic Serve as well pdate, in some o er acces Base Sco 7 and Int Vector: V/AC:L/ L/A:N).	r as nsert or f Oracle sible re 5.5 cegrity PR:H/U				
Improper Access Control	23-07-2019	7.5	Vulnera WebLog of Oracl (subcor Contain version 12.2.1.3 vulnera unauthe networ Server. this vul takeove Server. 9.8 (Con	ability in gic Serve nponent er - Java s that ar 3.0. Easil bility al enticate k access mise Or Success nerabili er of Ora CVSS 3.0 nfidentia ailability 5.0/AV:N /C:H/I:H	n the Ora er comp n Middle t: Applic aEE). Su re affect ly exploi lows d attack via T3 f racle We ful attac ty can re ful attac ty can re acle Web 0 Base S ality, Int v impact V/AC:L/ H/A:H).	acle onent eware cation pported ed is itable er with to ebLogic eks of esult in oLogic core core segrity s). CVSS	N/A		A-ORA- 130819	
peoplesoft_	enterprise_pe	opletoo	ols							
Informatio n Exposure	23-07-2019	4	Vulnera Enterpr compor PeopleS (subcor Wizard)	rise PT F nent of C Soft Proc nponent	PeopleTo Dracle ducts t: Pagelo	et	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 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
			and 8.5 vulnera privileg networ compre Enterp Success vulnera unauth data or People CVSS 3 (Confic Vector; (CVSS:: :N/S:U)	:	v exploit lows low cker wit via HT eopleSof PeopleTe cks of th an result ccess to te acces erprise l cessible Score 6.! v impact V/AC:L/ I/A:N).	able W h TP to t ools. is t in critical s to all PT data. 5 cs). CVSS PR:L/UI				
Improper Access Control	23-07-2019	4.9	Vulner Enterp compo People (subco Server) that ard and 8.5 vulnera priviles networ compre Enterp While t People signific product this vu unauth deletio	ability ir rise PT I nent of (Soft Pro- mponen). Suppo: e affecte 57. Diffic ability al ged attac rise PT I the vulne Soft Ente Tools, at cantly im cts. Succe lnerabili	n the Peo PeopleTe Dracle ducts t: Applid rted ver d are 8.9 ult to ex lows low cker wit copleSof PeopleSof PeopleSof PeopleTe erability erprise l tacks m spact ad essful at ty can r reation, dificatio	opleSoft ools cation sions 55, 8.56 ploit w h TP to t ools. r is in PT ay ditional tacks of esult in	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			People well as access People CVSS 3 (Confic impact (CVSS:: I:N/S:C	Soft Ente Tools ac unauthe to a subs Soft Ente Tools ac .0 Base S lentiality s). CVSS 3.0/AV:N C/C:L/I:H	cessible prized re set of erprise I cessible Score 7.1 y and Int Vector: V/AC:H/ I/A:N).	data as ead PT data. cegrity PR:L/U				
Improper Access Control	23-07-2019	5.8	Vulner Enterp compo People (subco Guide), that are and 8.5 vulnera unauth networ compre Enterp Success human person and wh in People signific produc this vul unauth delete a People well as access	ability ir rise Peo nent of (Soft Pro- mponen . Suppor e affecte 57. Easily ability al enticate somise Peo rise Peo sful attac interact other the nile the v oleSoft E Tools, at cantly im cts. Succe lnerabili orized u access to Soft Ente to a subs Soft Ente	a the Peo pleTools Dracle ducts t: Activit ted vers d are 8.5 7 exploit lows d attacks copleSof pleTools cks requi- cion from an the a rulnerab nterprise ttacks m pact adde essful att ty can re- pdate, in o some o erprise cessible porized re- set of	opleSoft s ty ions 55, 8.56 able er with CP to t s. ire n a ttacker ility is re ay ditional tacks of esult in nsert or f data as	N/A		A-ORA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U I:R/S:C/C:L/I:L/A:N).		
			CVE ID : CVE-2019-2772		
enterprise_	manager_ops_	center			
Improper Access Control	23-07-2019	4	Vulnerability in the Enterprise Manager Ops Center component of Oracle Enterprise Manager Products Suite (subcomponent: Networking). Supported versions that are affected are 12.3.3 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager Ops Center. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager Ops Center accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:L/A:N). CVE ID : CVE-2019-2728	N/A	A-ORA-ENTE- 130819/438
otcms					
otcms Improper Neutralizat ion of Input During	19-07-2019	4.3	OTCMS 3.81 allows XSS via the mode parameter in an apiRun.php?mudi=autoRun request.	N/A	A-OTC-OTCM- 130819/439
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			CVE ID : CVE-2019-13971		
Ovidentia					I
ovidentia					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	19-07-2019	3.5	index.php in Ovidentia 8.4.3 has XSS via tg=groups, tg=maildoms&idx=create&use rid=0&bgrp=y, tg=delegat, tg=site&idx=create, tg=site&item=4, tg=admdir&idx=mdb&id=1, tg=notes&idx=Create, tg=admfaqs&idx=Add, or tg=admoc&idx=addoc&item=. CVE ID : CVE-2019-13977	N/A	A-OVI-OVID- 130819/440
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	19-07-2019	6.5	Ovidentia 8.4.3 has SQL Injection via the id parameter in an index.php?tg=delegat&idx=me m request. CVE ID : CVE-2019-13978	N/A	A-OVI-OVID- 130819/441
palletsproje	ects				•
flask					
N/A	17-07-2019	5	The Pallets Project Flask before 1.0 is affected by: unexpected memory usage. The impact is: denial of service. The attack vector is: crafted encoded JSON data. The fixed version is: 1. CVE ID : CVE-2019-1010083	https://ww w.palletspr ojects.com/ blog/flask- 1-0- released/	A-PAL-FLAS- 130819/442
Pango					<u> </u>
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pango					
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-07-2019	7.5	Gnome Pango 1.42 and later is affected by: Buffer Overflow. The impact is: The heap based buffer overflow can be used to get code execution. The component is: function name: pango_log2vis_get_embedding _levels, assignment of nchars and the loop condition. The attack vector is: Bug can be used when application pass invalid utf-8 strings to functions like pango_itemize. CVE ID : CVE-2019-1010238	N/A	A-PAN-PANG- 130819/443
phpcoo					
oecms					
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	OECMS v4.3.R60321 and v4.3 later is affected by: Cross Site Request Forgery (CSRF). The impact is: The victim clicks on adding an administrator account. The component is: admincp.php. The attack vector is: network connectivity. The fixed version is: v4.3. CVE ID : CVE-2019-1010112	N/A	A-PHP-OECM- 130819/444
pivotal_soft	ware				
cloud_found	lry_uaa				
Improper Input Validation	18-07-2019	4.3	Cloud Foundry UAA, versions prior to v73.4.0, does not set an X-FRAME-OPTIONS header on various endpoints. A remote user can perform clickjacking attacks on UAA's frontend sites. CVE ID : CVE-2019-3794	https://wv w.cloudfou ndry.org/b og/cve- 2019-3794	A-PIV-CLOU- 130819/445
	cale 0.1				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pluck-cms		<u> </u>		[
pluckcms					
Unrestricte d Upload of File with Dangerous Type	16-07-2019	7.5	PluckCMS 4.7.4 and earlier is affected by: CWE-434 Unrestricted Upload of File with Dangerous Type. The impact is: get webshell. The component is: data/inc/images.php line36. The attack vector is: modify the MIME TYPE on HTTP request to upload a php file. The fixed version is: after commit 09f0ab871bf633973cfd9fc4fe 59d4a912397cf8.	N/A	A-PLU-PLUC- 130819/446
			CVE ID : CVE-2019-1010062		
premiumso	ftware				
cleditor					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	19-07-2019	4.3	Premium Software CLEditor 1.4.5 and earlier is affected by: Cross Site Scripting (XSS). The impact is: An attacker might be able to inject arbitrary html and script code into the web site. The component is: jQuery plug-in. The attack vector is: the victim must open a crafted href attribute of a link (A) element. CVE ID : CVE-2019-1010113	N/A	A-PRE-CLED- 130819/447
Proftpd					
proftpd					
Improper Access Control	19-07-2019	7.5	An arbitrary file copy vulnerability in mod_copy in ProFTPD up to 1.3.5b allows for remote code execution and information disclosure	N/A	A-PRO-PROF- 130819/448
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 213	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without authentication, a related issue to CVE-2015- 3306.		
			CVE ID : CVE-2019-12815		
Qbittorrent					
qbittorrent				1	
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	17-07-2019	7.5	In qBittorrent before 4.1.7, the function Application::runExternalProgr am() located in app/application.cpp allows command injection via shell metacharacters in the torrent name parameter or current tracker parameter, as demonstrated by remote command execution via a crafted name within an RSS feed. CVE ID : CVE-2019-13640	N/A	A-QBI-QBIT- 130819/449
quake3e_pr	oject				
quake3e					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-07-2019	7.5	Quake3e < 5ed740d is affected by: Buffer Overflow. The impact is: Possible code execution and denial of service. The component is: Argument string creation. CVE ID : CVE-2019-1010043	N/A	A-QUA-QUAK- 130819/450
rangerstudi					
directus_7_a	api				
Unrestricte d Upload of File with Dangerous Type	19-07-2019	6.8	In Directus 7 API through 2.3.0, uploading of PHP files is blocked only when the Apache HTTP Server is used, leading to uploads/_/originals remote	N/A	A-RAN-DIRE- 130819/451
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution with nginx.		
			CVE ID : CVE-2019-13980		
Improper Input Validation	19-07-2019	5	In Directus 7 API through 2.3.0, remote attackers can read image files via a direct request for a filename under the uploads/_/originals/ directory. This is related to a configuration option in which the file collection can be non- public, but this option does not apply to the thumbnailer. CVE ID : CVE-2019-13981	N/A	A-RAN-DIRE- 130819/452
directus_7			CVE ID : CVE-2019-13901		
unectus_/			interfaces/markdown/input.v		
Informatio n Exposure	19-07-2019	5	ue in Directus 7 Application before 7.7.0 does not sanitize Markdown text before rendering a preview. CVE ID : CVE-2019-13982	N/A	A-RAN-DIRE- 130819/453
rdbrck					
shift					
Improper Authentica tion	17-07-2019	5	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application. CVE ID : CVE-2019-12911	https://sup port.tryshif t.com/kb/a rticle/206- shift-34- released- on- january- 23-2019/	A-RDB-SHIF- 130819/454
Untrusted Search Path	17-07-2019	2.1	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application. CVE ID : CVE-2019-12912	https://sup port.tryshif t.com/kb/a rticle/206- shift-34- released- on-	A-RDB-SHIF- 130819/455
CV Scoring So (CVSS)	cale 0-1	1-2	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		
							januai 23-20	-		
N/A	17-07-2019	2.1	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application. CVE ID : CVE-2019-12913				https://sup port.tryshif t.com/kb/a rticle/206- shift-34- released- on- january- 23-2019/		A-RDB-SHIF- 130819/456	
Improper Authentica tion	17-07-2019	5	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application. CVE ID : CVE-2019-12914				https://sup port.tryshif t.com/kb/a rticle/206- shift-34- released- on- january- 23-2019/		A-RDB-SHIF- 130819/457	
Informatio n Exposure	17-07-2019	5	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application. CVE ID : CVE-2019-8931				https://sup port.tryshif t.com/kb/a rticle/206- shift-34- released- on- january- 23-2019/		A-RDB-SHIF- 130819/458	
Improper Authentica tion	17-07-2019	5	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application. CVE ID : CVE-2019-8932			https://sup port.tryshif t.com/kb/a rticle/206- shift-34- released- on- january- 23-2019/		A-RDB-SHIF- 130819/459		
Saltstack										
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	<mark>3-4</mark> 216	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
salt_2019		•			
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	18-07-2019	7.5	SaltStack Salt 2018.3, 2019.2 is affected by: SQL Injection. The impact is: An attacker could escalate privileges on MySQL server deployed by cloud provider. It leads to RCE. The component is: The mysql.user_chpass function from the MySQL module for Salt (https://github.com/saltstack /salt/blob/develop/salt/modu les/mysql.py#L1462). The attack vector is: specially crafted password string. The fixed version is: 2018.3.4. CVE ID : CVE-2019-1010259	N/A	A-SAL-SALT- 130819/460
salt_2018					
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	18-07-2019	7.5	SaltStack Salt 2018.3, 2019.2 is affected by: SQL Injection. The impact is: An attacker could escalate privileges on MySQL server deployed by cloud provider. It leads to RCE. The component is: The mysql.user_chpass function from the MySQL module for Salt (https://github.com/saltstack /salt/blob/develop/salt/modu les/mysql.py#L1462). The attack vector is: specially crafted password string. The fixed version is: 2018.3.4. CVE ID : CVE-2019-1010259	N/A	A-SAL-SALT- 130819/461
scapy					
scapy					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				217						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontroll ed Resource Consumpti on	19-07-2019	5	scapy 2.4.0 is affected by: Denial of Service. The impact is: infinite loop, resource consumption and program unresponsive. The component is: _RADIUSAttrPacketListField.ge tfield(self). The attack vector is: over the network or in a pcap. both work. CVE ID : CVE-2019-1010142	N/A	A-SCA-SCAP- 130819/462
send-anywl	here				
send_anywl	here				
N/A	22-07-2019	4	The Send Anywhere application 9.4.18 for Android stores confidential information insecurely on the system (i.e., in cleartext), which allows a non-root user to find out the username/password of a valid user via /data/data/com.estmob.andro id.sendanywhere/shared_pref s/sendanywhere_device.xml. CVE ID : CVE-2019-13100	N/A	A-SEN-SEND- 130819/463
sertek					
xpare					
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-07-2019	10	An issue was discovered in Sertek Xpare 3.67. The login form does not sanitize input data. Because of this, a malicious agent could access the backend database via SQL injection. CVE ID : CVE-2019-13447	N/A	A-SER-XPAR- 130819/464
Improper	17-07-2019	4.3	An issue was discovered in	N/A	A-SER-XPAR-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 218	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	n	NCIIPC ID
Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') servicestac			Sertek Xpare 3.67. The login form does not sanitize input data. Because of this, a malicious agent could exploit the vulnerable function in order to prepare an XSS payload to send to the product's clients. CVE ID : CVE-2019-13448			130819/465
servicestac	k					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-07-2019	4.3	ServiceStack ServiceStack Framework 4.5.14 is affected by: Cross Site Scripting (XSS). The impact is: JavaScrpit is reflected in the server response, hence executed by the browser. The component is: the query used in the GET request is prone. The attack vector is: Since there is no server-side validation and If Browser encoding is bypassed, the victim is affected when opening a crafted URL. The fixed version is: 5.2.0. CVE ID : CVE-2019-1010199	N/A		A-SER-SERV- 130819/466
Sitecore						
experience_	platform					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	3.5	In Sitecore 9.0 rev 171002, Persistent XSS exists in the Media Library and File Manager. An authenticated unprivileged user can modify the uploaded file extension parameter to inject arbitrary JavaScript. CVE ID : CVE-2019-13493	N/A		A-SIT-EXPE- 130819/467
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sleuthkit	I				
the_sleuth_	kit				
Integer Overflow or Wraparou nd	18-07-2019	4.3	The Sleuth Kit 4.6.0 and earlier is affected by: Integer Overflow. The impact is: Opening crafted disk image triggers crash in tsk/fs/hfs_dent.c:237. The component is: Overflow in fls tool used on HFS image. Bug is in tsk/fs/hfs.c file in function hfs_cat_traverse() in lines: 952, 1062. The attack vector is: Victim must open a crafted HFS filesystem image. CVE ID : CVE-2019-1010065	N/A	A-SLE-THE 130819/468
			CVE ID : CVE-2019-1010065		
Status					
react_native	e_desktop				
Improper Input Validation	23-07-2019	7.5	ubuntu-server.js in Status React Native Desktop before v0.57.8_mobile_ui allows Remote Code Execution. CVE ID : CVE-2019-12164	https://git hub.com/st atus- im/react- native- desktop/p ull/475/co mmits/f69 45f1e4b15 7c69e414c d94fe5cde 1876aabcc 1	A-STA-REAC- 130819/469
Sweetscape					
010_editor					
Improper Input Validation	22-07-2019	5.8	In SweetScape 010 Editor 9.0.1, improper validation of arguments in the internal implementation of the Memcpy function (provided by	N/A	A-SWE-010 130819/470
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the scripting engine) allows an attacker to overwrite arbitrary memory, which could lead to code execution.		
			CVE ID : CVE-2019-12551		
Integer Overflow or Wraparou nd	22-07-2019	4.3	In SweetScape 010 Editor 9.0.1, an integer overflow during the initialization of variables could allow an attacker to cause a denial of service.	N/A	A-SWE-010 130819/471
			CVE ID : CVE-2019-12552		
	k_a5_project				
syguestboo	k_a5		SyGuestBook A5 Version 1.2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	18-07-2019	allows stored XSS because the isValidData function in include/functions.php does		N/A	A-SYG-SYGU- 130819/472
Scripting')			CVE ID : CVE-2019-13948		
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	SyGuestBook A5 Version 1.2 has no CSRF protection mechanism, as demonstrated by CSRF for an index.php?c=Administrator&a =update admin password change. CVE ID : CVE-2019-13949	N/A	A-SYG-SYGU- 130819/473
Improper Neutralizat ion of Input During Web Page Generation	18-07-2019	3.5	index.php?c=admin&a=index in SyGuestBook A5 Version 1.2 has stored XSS via a reply to a comment. CVE ID : CVE-2019-13950	N/A	A-SYG-SYGU- 130819/474
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Tcpdump	L				
tcpdump					
Out-of- bounds Read	22-07-2019	4.3	tcpdump.org tcpdump 4.9.2 is affected by: CWE-126: Buffer Over-read. The impact is: May expose Saved Frame Pointer, Return Address etc. on stack. The component is: line 234: "ND_PRINT((ndo, "%s", buf));", in function named "print_prefix", in "print- hncp.c". The attack vector is: The victim must open a specially crafted pcap file. CVE ID : CVE-2019-1010220	N/A	A-TCP-TCPD- 130819/475
techytalk				<u> </u>	
quick_chat					
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	18-07-2019	7.5	TechyTalk Quick Chat WordPress Plugin All up to the latest is affected by: SQL Injection. The impact is: Access to the database. The component is: like_escape is used in Quick-chat.php line 399. The attack vector is: Crafted ajax request. CVE ID : CVE-2019-1010104	N/A	A-TEC-QUIC- 130819/476
temenos					
CWX					
Improper Access Control	17-07-2019	5	Temenos CWX version 8.9 has an Broken Access Control vulnerability in the module /CWX/Employee/EmployeeEd it2.aspx, leading to the viewing of user information.	N/A	A-TEM-CWX- 130819/477
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pa	tch	NCIIP	PC ID
			CVE ID	: CVE-2	019-13	403				
timesheet_r	next_gen_proje	ect	<u> </u>				_ I			
timesheet_r	next_gen									
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	earlier Site Scr impact to exec JavaScr parame Web lo lines 40 vector may cli	via a "r	ross e tacker "ML and edirect" nent is: ohp, tack , victim s url.	N/A		A-TIM-7 130819		
tiny.cloud										
tinymce										
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	affected Neutra Web Pa impact executi Media o vector paste n media o	tinymce 4.7.11, 4.7.12 is affected by: CWE-79: Improper Neutralization of Input During Web Page Generation. The impact is: JavaScript code execution. The component is: Media element. The attack vector is: The victim must paste malicious content to media element's embed tab. CVE ID : CVE-2019-1010091					A-TIN-7 130819	
tronlink										
wallet N/A	22-07-2019	5	TronLink Wallet 2.2.0 stores user wallet keystore in plaintext and places them in insecure storage. An attacker can read and reuse the user keystore of a valid user via /data/data/com.tronlink.walle t/shared_prefs/ <wallet-< td=""><td>N/A</td><td></td><td>A-TRO- 130819</td><td></td></wallet-<>				N/A		A-TRO- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish D	Date	CVSS	Description & CVE ID				Pat	tch	NCIIF	PC ID
				unauth	xml to ۽ orized a : CVE-2	-	096				
Informatio n Exposure Through Log Files	22-07-20)19	4	registr Wallet when t Create called. users c later. T read us device. prior to Bean), sandbo any ap the dev read da applica	ation for 2.2.0 is the class WalletT Other an can read the logge sing Log When u o Andro the log o oxed per plication vice has ata logge	woActiv uthentic it in the ed data o cat on th using pla id 4.1 (Je data is n applica n installe	onLink n the log ity is ated log can be te tforms elly ot tion; ed on bility to ner	N/A		A-TRO- 130819	
univention				<u>.</u>							
univention_	corporate	e_ser	ver								
Informatio n Exposure	17-07-20)19	5	Univention Corporate Server univention-directory-notifier 12.0.1-3 and earlier is affected by: CWE-213: Intentional Information Exposure. The impact is: Loss of Confidentiality. The component is: function data_on_connection() in src/callback.c. The attack vector is: network connectivity. The fixed version is: 12.0.1-4 and later. CVE ID : CVE-2019-1010283				N/A		A-UNI-0 130819	
upwork			-	•							
CV Scoring So	cale	-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				22/						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
time_tracke	er				
N/A	23-07-2019	4.6	Upwork Time Tracker 5.2.2.716 doesn't verify the SHA256 hash of the downloaded program update before running it, which could lead to code execution or loca privilege escalation by replacing the original update.exe. CVE ID : CVE-2019-12162	d N/A	A-UPW-TIME- 130819/483
vcftools_pro	niect				
vcftools	Jeee				
VCILOUIS					
Use After Free	25-07-2019	6.8	VCFTools vcftools prior to version 0.1.15 is affected by: Use-after-free. The impact is: Denial of Service or possibly other impact (eg. code execution or information disclosure). The component i The header::add_FILTER_descript r method in header.cpp. The attack vector is: The victim must open a specially crafted VCF file. CVE ID : CVE-2019-101012	s: https://git hub.com/v cftools/vcft ools/issues /141	A-VCF-VCFT- 130819/484
Veeam					
one_reporte	er				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-07-2019	3.5	Veeam ONE Reporter 9.5.0.3201 allows XSS via the Add/Edit Widget with a crafted Caption field to setDashboardWidget in CommonDataHandlerReadOr y.ashx. CVE ID : CVE-2019-14297	N/A	A-VEE-ONE 130819/485
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	27-07-2019	3.5	Veeam ONE Reporter 9.5.0.3201 allows XSS via a crafted Description(config) field to addDashboard or editDashboard in CommonDataHandlerReadOnl y.ashx. CVE ID : CVE-2019-14298	N/A	A-VEE-ONE 130819/486
Videolan	L				
vlc_media_p	olayer				
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-07-2019	4.3	libebml before 1.3.6, as used in the MKV module in VideoLAN VLC Media Player binaries before 3.0.3, has a heap-based buffer over-read in EbmlElement::FindNextEleme nt. CVE ID : CVE-2019-13615	N/A	A-VID-VLC 130819/487
Out-of- bounds Read	18-07-2019	7.5	lavc_CopyPicture in modules/codec/avcodec/vide o.c in VideoLAN VLC media player through 3.0.7 has a heap-based buffer over-read because it does not properly validate the width and height. CVE ID : CVE-2019-13962	N/A	A-VID-VLC 130819/488
wcms					
wcms					
Cross-Site Request Forgery (CSRF)	23-07-2019	5.8	WCMS v0.3.2 has a CSRF vulnerability, with resultant directory traversal, to modify index.html via the /wex/html.php?finish=/index .html URI. CVE ID : CVE-2019-14240	N/A	A-WCM- WCMS- 130819/489
webappick					
CV Scoring So (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
woocomme	rce_product_fe	eed			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-07-2019	4.3	WebAppick WooCommerce Product Feed 2.2.18 and earlier is affected by: Cross Site Scripting (XSS). The impact is: XSS to RCE via editing theme files in WordPress. The component is: admin/partials/woo-feed- manage-list.php:63. The attack vector is: Administrator must be logged in. CVE ID : CVE-2019-1010124		A-WEB- WOOC- 130819/490
Wireshark					
wireshark					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-07-2019	5	In Wireshark 3.0.0 to 3.0.2, 2.6.0 to 2.6.9, and 2.4.0 to 2.4.15, the ASN.1 BER dissector and related dissectors could crash. This was addressed in epan/asn1.c by properly restricting buffer increments. CVE ID : CVE-2019-13619	N/A	A-WIR-WIRE- 130819/491
wp-code-hi	 ghlightjs_proje	ect			
wp-code-hi	ghlightjs				
Cross-Site Request Forgery (CSRF)	19-07-2019	6.8	An issue was discovered in the wp-code-highlightjs plugin through 0.6.2 for WordPress. wp-admin/options- general.php?page=wp-code- highlight-js allows CSRF, as demonstrated by an XSS payload in the hljs_additional_css parameter. CVE ID : CVE-2019-12934	N/A	A-WPWP-C- 130819/492
wpeverest	I				I
CV Scoring S (CVSS)	cale 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 & CVE ID			Pa	tch	NCIIP	PC ID	
everest_for	ms										
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	18-0	7-2019	7.5	A SQL injection vulnerability exists in WPEverest Everest Forms plugin for WordPress through 1.4.9. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system via includes/evf-entry- functions.php CVE ID : CVE-2019-13575				N/A		A-WPE- 130819	
Zammad											
Zammad											
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	16-0	7-2019	4.3	and ea Cross S CWE-8 Execut users b is: web is: the ticket.	Zammad GmbH Zammad 2.3.0 and earlier is affected by: Cross Site Scripting (XSS) - CWE-80. The impact is: Execute java script code on users browser. The component is: web app. The attack vector is: the victim must open a ticket. The fixed version is: 2.3.1, 2.2.2 and 2.1.3.			N/A		A-ZAM- ZAMM- 130819	
zeek											
zeek											
NULL Pointer Dereferenc e	17-0	7-2019	5	In Zeek Network Security Monitor (formerly known as Bro) before 2.6.2, a NULL pointer dereference in the Kerberos (aka KRB) protocol parser leads to DoS because a case-type index is mishandled. CVE ID : CVE-2019-12175				om/z eek/r es/tag	A-ZEE-2 130819		
Zohocorp	<u> </u>							<u> </u>		I	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
manageeng	ine_adselfserv	ice_plu	15		
N/A	17-07-2019	8.5	Zoho ManageEngine ADManager Plus 6.6.5, ADSelfService Plus 5.7, and DesktopCentral 10.0.380 have Insecure Permissions, leading to Privilege Escalation from low level privileges to System. CVE ID : CVE-2019-12876	N/A	A-ZOH- MANA- 130819/496
manageeng	ine_admanage	r_plus			
N/A	17-07-2019	8.5	Zoho ManageEngine ADManager Plus 6.6.5, ADSelfService Plus 5.7, and DesktopCentral 10.0.380 have Insecure Permissions, leading to Privilege Escalation from low level privileges to System. CVE ID : CVE-2019-12876	N/A	A-ZOH- MANA- 130819/497
manageeng	ine_desktop_c	entral			
N/A	17-07-2019	8.5	Zoho ManageEngine ADManager Plus 6.6.5, ADSelfService Plus 5.7, and DesktopCentral 10.0.380 have Insecure Permissions, leading to Privilege Escalation from low level privileges to System. CVE ID : CVE-2019-12876	N/A	A-ZOH- MANA- 130819/498
zzcms					
zzmcms					
Improper Access Control	19-07-2019	7.5	zzcms zzmcms 8.3 and earlier is affected by: File Delete to getshell. The impact is: getshell. The component is: /user/ppsave.php. CVE ID : CVE-2019-1010151	N/A	A-ZZC-ZZMC- 130819/499
zzcms			L	<u> </u>	

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				220						

Weakness	Publish Date	CVSS	Description & CVE I) Pa	tch	NCIIP	CID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	23-07-2019	7.5	zzcms version 8.3 and ea is affected by: SQL Inject The impact is: zzcms File Delete to Code Execution CVE ID : CVE-2019-101	ion. e N/A n.		A-ZZC-Z 130819	
Improper Input Validation	23-07-2019	7.5	zzcms version 8.3 and ea is affected by: File Delete Code Execution. The imp zzcms File Delete to Cod Execution. The compone user/licence_save.php. CVE ID : CVE-2019-101	e to bact is: e N/A ent is:		A-ZZC-Z 130819	
Improper Input Validation	23-07-2019	7.5	zzcms 8.3 and earlier is affected by: File Delete to Execution. The impact is getshell. The component /user/zssave.php. CVE ID : CVE-2019-101	:: is: N/A		A-ZZC-Z 130819	
Improper Input Validation	23-07-2019	7.5	zzcms 8.3 and earlier is affected by: File Delete to Execution. The impact is getshell. The component user/manage.php line 3 CVE ID : CVE-2019-101	:: : is: N/A 1-80.		A-ZZC-Z 130819	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	23-07-2019	7.5	zzcms 8.3 and earlier is affected by: SQL Injectio impact is: sql inject. The component is: zs/subzs. CVE ID : CVE-2019-101	php.		A-ZZC-Z 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 230	5-6 6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pa	tch	NCIIP	PC ID
			Ope	erating	System				1	
akuvox										
sp-r50p_fir	mware									
Use of Hard- coded Credential s	22-07-2019	10	Akuvox 50.0.6.1 get acco telnet.7 running cannot credent	Hardcoded credentials in the Akuvox R50P VoIP phone 50.0.6.156 allow an attacker to get access to the device via telnet. The telnet service is running on port 2323; it cannot be turned off and the credentials cannot be changed. CVE ID : CVE-2019-12327					0-AKU- 130819	
Atcom							•			
a10w_firmw	ware									
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	22-07-2019	9	input v remote configu interfac VoIP ph 2.6.1a2 authent in the s OS com metach	A command injection (missing input validation) issue in the remote phonebook configuration URI in the web interface of the Atcom A10W VoIP phone with firmware 2.6.1a2421 allows an authenticated remote attacker in the same network to trigger OS commands via shell metacharacters in a POST request.			N/A		0-ATC-/ 130819	
Canonical	I								<u> </u>	
ubuntu_linu	ıx									
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker			N/A		0-CAN- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2737		
Improper Access Control	23-07-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Compiling). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/U I:N/S:U/C:L/I:N/A:N).	N/A	0-CAN-UBUN- 130819/508
Improper Access Control	23-07-2019	3.6	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent:	N/A	O-CAN-UBUN- 130819/509
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	PC ID
			Suppor affected 5.7.26 a and pri vulnera privileg to the i MySQL compro Success vulnera unauth hang or crash (f MySQL unauth delete a MySQL CVSS 3 (Integr impacta (CVSS:3 :N/S:U)	Security rted vers d are 5.6 and prio ior. Easil ability al ged attac nfrastru Server e omise My sful attac ability ca ability ca ability ca complete Server a orized u access to Server a orized u access to Server a .0 Base S rity and A s). CVSS 3.0/AV:L /C:N/I:L	sions tha 5.44 and 6.44 and 9.44 and 9.44 and 9.44 and 9.45 10.45	at are prior, 0.16 table gh h logon here s to rver. is cause a eatable of is nsert or f le data. L ity PR:H/UI				
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: XML). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable			N/A		0-CAN- 130819		
I										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:N/A:H).		
			CVE ID : CVE-2019-2740		
Improper Access Control	23-07-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Log). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2741	N/A	0-CAN-UBUN- 130819/511
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via	N/A	O-CAN-UBUN- 130819/512
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:N/I:L/A:L).		
Improper Access Control	23-07-2019	5.5	CVE ID : CVE-2019-2778 Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U	N/A	O-CAN-UBUN- 130819/513

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				225						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch		NCIIP	C ID
			I:N/S:U/C:L/I:L/A:N).				
			CVE ID : CVE-2019-2791				
Improper Access Control	23-07-2019	2.3	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2797	N/A		0-CAN-1 130819	
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability	N/A		0-CAN-1 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2757		
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:L/A:H). CVE ID : CVE-2019-2758	N/A	0-CAN-UBUN- 130819/516
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported	N/A	O-CAN-UBUN- 130819/517
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:N/A:H).		
Improper Access Control	23-07-2019	4	CVE ID : CVE-2019-2774 Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI	N/A	0-CAN-UBUN- 130819/518

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				220						

Improper Access Control 23-07-2019 5.5 Server component of MSQL Server component: Server: Security: Audit). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U EN/S:U/C:N/I:L/A:H). CVE ID : CVE-2019-2819 https://ww wilbreoffic e.org/abou to/Security /advisories /CVE. Improper Input Validation 17-07-2019 7.5 LibreOffice has a feature where documents can specify that pre-installed scripts can be executed on various document events such as mouse-over, etc. LibreOffice is typically also bundled with LibreLogo, a programmable turtle vector graphics script, which can be manipulated into https://ww validation	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control23-07-20195.5Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 80.16 and prior. Easily exploitable whilerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/1:L/A:H). CVE ID : CVE-2019-2819https://ww wilbreoffic e.org/abou t- us/socurity /advisories /CVE- 2019-9848https://ww valuality/socurity /advisories /CVE- 2019-9848				:N/S:U/C:N/I:N/A:H).		
Improper Access Control23-07-20195.5Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS 				CVE ID : CVE-2019-2805		
Improper Input Validation17-07-20197.5where documents can specify that pre-installed scripts can be executed on various document events such as mouse-over, etc. LibreOffice is typically also bundled with LibreLogo, a programmable turtle vector graphics script, which can be manipulated intohttps://ww w.libreoffic e.org/abou0-CAN-UBUN- 130819/520	Access	23-07-2019	5.5	Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U I:N/S:U/C:N/I:L/A:H). CVE ID : CVE-2019-2819		
CV Scoring Scale	Input	17-07-2019	7.5	where documents can specify that pre-installed scripts can be executed on various document events such as mouse-over, etc. LibreOffice is typically also bundled with LibreLogo, a programmable turtle vector graphics script,	w.libreoffic e.org/abou t- us/security /advisories /CVE- 2019-9848	c 1 0-CAN-UBUN- y 130819/520 s
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	-	cale 0-1	1-2	2 -3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Descripti	ion & CVE I	D	Pat	tch	NCIIP	CID
			executing arbi commands. By document eve trigger LibreLd python contain document a m document a m document cou constructed w execute arbitra commands sile warning. In th LibreLogo can from a docume handler. This i Document Fou LibreOffice ver 6.2.5.						
Informatio n Exposure	17-07-2019	4	LibreOffice has mode' in which documents from deemed 'trustof to retrieve rem This mode is m mode, but can users who wan LibreOffice's a remote resour document. A fl where bullet g omitted from to prior to version issue affects: E Foundation Li versions prior CVE ID : CVE- 2	s a 'stealth h only om locatio ed' are all note resound note resound the enable not the def be enable not to disab ubility to in ces within law existe graphics within this prote on 6.2.5. The Document breOffice	h ns owed urces. fault ed by ole nclude n a d vere ction his	https:, w.libr e.org/ t- us/sec /advis /CVE- 2019-	eoffic abou curity sories	0-CAN- 130819	
chinamobile	eltd								
gpn2.4p21-	c-cn_firmware	,							
Improper	19-07-2019	7.8	ChinaMobile GPN2.4P21-C-CN			N/A		O-CHI-C	SPN2-
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access Control			W2001EN-00 is affected by: Incorrect Access Control - Unauthenticated Remote Reboot. The impact is: PLC Wireless Router's are vulnerable to an unauthenticated remote reboot due. The component is: Reboot settings are available to unauthenticated users instead of only authenticaed users. The attack vector is: Remote.		130819/522
Cisco			CVE ID : CVE-2019-1010136		
	p_firmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.	N/A	0-CIS-SG50- 130819/523

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

	Publish Date	CVSS	Description & CVE ID				tch	NCIIP	PCID
			CVE ID : CVE-2019-1943						
sg500-52p_f	firmware								
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943		N/A		0-CIS-S 130819		
sg500x-24_f			A vulnerability	in the use	h				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP			N/A		0-CIS-S 130819	
CV Scoring Sc (CVSS)	ale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE	ID	Pat	ch	NCIIP	CID
			request and modifying request that causes th interface to redirect th to a specific malicious This type of vulnerabi known as an open red attack and is used in p attacks that get users to unknowingly visit mal sites. CVE ID : CVE-2019-19					
sg500x-24p	_firmware							
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the v interface of Cisco Sma Business 200, 300, and Series Switches softwa allow an unauthentica remote attacker to red user to a malicious we The vulnerability is du improper input valida the parameters of an H request. An attacker co exploit this vulnerabil intercepting a user's H request and modifying request that causes th interface to redirect th to a specific malicious This type of vulnerabil known as an open red attack and is used in p attacks that get users to unknowingly visit mal- sites. CVE ID : CVE-2019-19	II 1 500 are could ted, lirect a b page. le to tion of ITTP ould ity by ITTP g it into a le web le user URL. lity is irect hishing to icious	N/A		0-CIS-S 130819	
sg500x-48_			A uulnorability in the	woh			O-CIS-S	G50-
Redirectio	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small		N/A		130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 243	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIF	PC ID
n to Untrusted Site ('Open Redirect')			Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943				
sg500x-48p	_firmware						
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL.	N/A		0-CIS-S 130819	
CV Scoring S	cale 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	4-5	5-6	6-7	7-8	8-9	
				244						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.		
			CVE ID : CVE-2019-1943		
sg500xg-8f8	Bt_firmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SG50- 130819/529
spa500ds_fi	irmware				
Improper Neutralizat ion of Special Elements used in a	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The	N/A	O-CIS-SPA5- 130819/530
CV Scoring So (CVSS)	cale 0-1	1-2	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	PC ID
Command ('Comman d Injection')			vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. CVE ID : CVE-2019-1923				
spa500s_fir	mware						
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to	N/A		0-CIS-S 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 246	6-7	7-8	8-9	9-10

(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9
				246					

Weakness	Publi	ish Date	CVSS	ſ	Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
				execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. CVE ID : CVE-2019-1923							
spa501g_fir	mwar	·e		CVEID	CVE-2	.019-19	23				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	17-07	7-2019	4.6	Busine Phones physica to exect comma vulnera improp the dev interfa exploit accessi interfa passwo the dev and ins device. could a execute on the securit publica affecte SPA50 firmwa and pri	erability ss SPA5 s could a ally prox cute arbi ands on f ability is per inpu- vice conf ce. An at this vul ing the c ce, whic ord, and vice's ph serting a A succe allow the e arbitra device in ty contex ation, this d Cisco S are relea ior.	00 Serie llow a simate at trary the devic due to t validat iguratio tacker c nerabilit onfigura h may re then acc ysical in USB sto ssful exp e attacke ry comr n an elev st. At the is vulner Small Bu IP Phon ses 7.6.2	s IP ttacker ce. The ion in n ould ty by tion equire a cessing terface rage oloit r to nands vated time of vated time of vatess siness es 2SR5	N/A		0-CIS-S 130819	
spa502g_fir											
Improper	17-07	7-2019	4.6	A vulne	erability	in Cisco	Small	N/A		O-CIS-S	PA5-
CV Scoring So (CVSS)	ale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIP	CID
Neutralizat ion of Special Elements used in a Command ('Comman d Injection')			Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. CVE ID : CVE-2019-1923			130819	
spa504g_fir	mware						
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a	N/A		0-CIS-S 130819	
CV Scoring So (CVSS)	cale 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	[Descriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
				the device. and insidevice. could a execute on the securit publica affecte SPA50 firmwa and pri	vice's ph serting a A succe llow the e arbitra device in y contex ation, this d Cisco S D Series are relea	then acc ysical in USB sto ssful exj e attacke ary comr n an elev at. At the is vulner Small Bu IP Phon ses 7.6.2 2019-19	terface orage oloit er to nands vated time of rability siness es 2SR5				
spa508g_fir	mware			<u></u>				- H			
spa508g_firmware				A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones				N/A		0-CIS-S 130819	
CV Scoring So (CVSS)	cale 0-	-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-:
				249						

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIF	PC ID
			and pri	ior.						
			CVE ID) : CVE-2	2019-19	23				
spa509g_fir	mware		<u></u>				-		•	
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	17-07-2019	4.6	Busine Phones physica to exect comma vulnera improp the dev interfa exploit accessi interfa passwo the dev and ins device. could a execute on the securit publica affected SPA500 firmwa and pri	ation, thi d Cisco S 0 Series are relea	00 Serie llow a kimate a trary the devi due to t validat figuratio tacker o nerabili onfigura h may ro then acc ysical in USB sto ssful exp e attacke is vulner Small Bu IP Phon ses 7.6.2	s IP ttacker ce. The ion in on could ty by ation equire a cessing terface orage ploit er to nands vated e time of rability usiness es 2SR5	N/A		0-CIS-S 130819	
spa512g_fir	mware								1	
Improper Neutralizat ion of Special Elements used in a Command ('Comman	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in				N/A		0-CIS-S 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 250	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Injection')	ection')		the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior.		
			CVE ID : CVE-2019-1923		
spa514g_fir	mware				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated	N/A	O-CIS-SPA5- 130819/538

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				251						

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	Pa	tch	NCIIP	CID	
			publica affecte SPA50	y contex ation, thi d Cisco S 0 Series are relea ior.	s vulner Small Bu IP Phon					
			CVE ID) : CVE-2	019-19	23				
aironet_370	00e_firmware									
Improper Input Validation	17-07-2019	6.1	Fast Tr implem Access could a unauth attacke service affecte vulner comple conditi authen a targe for FT. exploit sendin requess interfa	A vulnerability in the 802.11r Fast Transition (FT) implementation for Cisco IOS Access Points (APs) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected interface. The vulnerability is due to a lack of complete error handling condition for client authentication requests sent to a targeted interface configured for FT. An attacker could exploit this vulnerability by sending crafted authentication request traffic to the targeted interface, causing the device to restart unexpectedly.					0-CIS-A 130819	
aironet_370	00i_firmware									
Improper Input Validation	17-07-2019	6.1	Fast Tr implen Access could a unauth attacke service	erability cansition nentatio Points (allow an nenticate er to cau e (DoS) c d interfa	(FT) n for Cis APs) So d, adjac se a den ondition	co IOS ftware ent ial of	N/A		0-CIS-A 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	2-3 3-4 4-5 5-6					8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a lack of complete error handling condition for client authentication requests sent to a targeted interface configured for FT. An attacker could exploit this vulnerability by sending crafted authentication request traffic to the targeted interface, causing the device to restart unexpectedly. CVE ID : CVE-2019-1920		
aironet 370	00p_firmware				
Improper Input Validation	17-07-2019	6.1	A vulnerability in the 802.11r Fast Transition (FT) implementation for Cisco IOS Access Points (APs) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected interface. The vulnerability is due to a lack of complete error handling condition for client authentication requests sent to a targeted interface configured for FT. An attacker could exploit this vulnerability by sending crafted authentication request traffic to the targeted interface, causing the device to restart unexpectedly. CVE ID : CVE-2019-1920	N/A	0-CIS-AIRO- 130819/541
spa525g2_f	irmware				
Improper Neutralizat ion of Special	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker	N/A	0-CIS-SPA5- 130819/542
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
Elements used in a Command ('Comman d Injection')			to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. CVE ID : CVE-2019-1923	mmands on the device. The Inerability is due to proper input validation in e device configuration cerface. An attacker could ploit this vulnerability by cessing the configuration cerface, which may require a ssword, and then accessing e device's physical interface d inserting a USB storage vice. A successful exploit uld allow the attacker to ecute arbitrary commands the device in an elevated curity context. At the time of blication, this vulnerability fected Cisco Small Business A500 Series IP Phones mware releases 7.6.2SR5 d prior.			
sf200-24_fin URL Redirectio n to Untrusted Site ('Open Redirect')	rmware 17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user	N/A	0-CIS-SF20- 130819/543		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7	² -8 8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	s type of vulnerability is own as an open redirect ack and is used in phishing acks that get users to knowingly visit malicious es.			
sf200-24fp_	firmware			_			
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SF20- 130819/544		
sf200-24p_f	irmware						
URL Redirectio n to Untrusted Site ('Open	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated,	N/A	0-CIS-SF20- 130819/545		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Redirect')Image: Redirect's and the set of the set o	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	ı	NCIIP	C ID
sf200-48_firmware sf200-48_firmware sf200-48_firmware state state <td>Redirect')</td> <td></td> <td></td> <td>user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.</td> <td></td> <td></td> <td></td> <td></td>	Redirect')			user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.				
URL Redirection n to Untrusted Setier ('Open Redirect')17-07-20195.8interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirectN/AO-CIS-SF20- 130819/546	sf200-48_fi	rmware						
	Redirectio n to Untrusted Site ('Open	17-07-2019	5.8	interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect	N/A			

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				256						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943		
sf200-48p_1	firmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	O-CIS-SF20- 130819/547
sf300-08_fi	rmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of	N/A	0-CIS-SF30- 130819/548
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	:h	NCIIF	PC ID
			the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943				
sf300-24_fi	rmware						
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A		0-CIS-S 130819	
CV Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	۱	NCIIPC ID
sf300-24mp	o_firmware					
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A		0-CIS-SF30- 130819/550
sf300-24p_f	firmware					
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a	N/A		0-CIS-SF30- 130819/551
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 259	6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943		
sf300-24pp	_firmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SF30- 130819/552
sf300-48_fi	rmware				
URL Redirectio n to	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500	N/A	0-CIS-SF30- 130819/553
CV Scoring So (CVSS)	cale 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
Untrusted Site ('Open Redirect')			allow a remote user to The vu improp the par reques exploit interce reques reques interfa to a spe This ty known attack a attacks unknow	Switches an unauth e attackes a malici lnerabili per input rameters t. An atta this vulue t and mo t that can ce to red ecific ma pe of vul as an op and is us that get wingly vi	henticat r to redi ous web ty is due validat of an H' acker co nerabilit user's H' odifying uses the licious I nerabilit een redin eed in ph users to isit mali	ed, rect a o page. e to ion of TTP uld cy by TTP it into a web e user JRL. ty is rect ishing o cious				
sf300-48p_1	firmware		A vulne	erahility	in the w	zeh			I 	
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is		N/A		0-CIS-S 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-
				261					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943		
sf300-48pp	firmwara		CVEID. CVE-2019-1943		
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SF30- 130819/555
sf302-08_fin	rmware		A local 11 to the sh		
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page.	N/A	0-CIS-SF30- 130819/556
CV Scoring So (CVSS)	cale 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	tch	NCIIF	PC ID
			The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943							
sf302-08mp	o_firmware									
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious		N/A		0-CIS-S 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	<mark>3-4</mark> 263	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1
				263						

Weakness	Publish Date	CVSS	Description & CV	'E ID	Pa	tch	NCIIP	C ID
			sites.					
			CVE ID : CVE-2019-1	943				
sf302-08mp	op_firmware							
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the interface of Cisco Sma Business 200, 300, ar Series Switches softwa allow an unauthentic remote attacker to re user to a malicious w The vulnerability is d improper input valid the parameters of an request. An attacker of exploit this vulnerability is intercepting a user's request and modifyin request that causes the interface to redirect to to a specific maliciou This type of vulnerability known as an open red attacks that get users unknowingly visit ma sites. CVE ID : CVE-2019-1	N/A		0-CIS-S 130819		
sf302-08p_f	firmware						_	
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the interface of Cisco Sma Business 200, 300, an Series Switches softw allow an unauthentic remote attacker to re user to a malicious w The vulnerability is d improper input valid the parameters of an request. An attacker of	N/A		0-CIS-S 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943		
sf302-08pp	_firmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SF30- 130819/560
sf500-24_fi	rmware				
CV Scoring S (CVSS)	cale 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	scriptio	on & CVE	ID	Pat	tch	NCIIF	PC ID
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943				N/A		0-CIS-S 130819	
sf500-24p_f	irmware		-						r	
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web				N/A		0-CIS-S 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.		
			CVE ID : CVE-2019-1943		
sf500-48_fi	rmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SF50- 130819/563
sf500-48p_1	irmware				
URL Redirectio n to Untrusted	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could	N/A	0-CIS-SF50- 130819/564
CV Scoring So (CVSS)	cale 0-1	1-2	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	PC ID
Site ('Open Redirect')			allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943				
sg200-08_fi	rmware						
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect	N/A		0-CIS-S 130819	
CV Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				268						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack and is used in phishing attacks that get users to unknowingly visit malicious sites.	5	
200.00			CVE ID : CVE-2019-1943		
sg200-08p_	firmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software cou allow an unauthenticated, remote attacker to redirect a user to a malicious web page The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SG20- 130819/566
sg200-10fp	firmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software cou allow an unauthenticated, remote attacker to redirect a user to a malicious web page The vulnerability is due to	N/A	0-CIS-SG20- 130819/567
CV Scoring So (CVSS)	cale 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	on & CVE	ID	Ра	tch	NCIIP	CID
			improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943							
ag200 10 f			CVE ID) : CVE- 2	2019-19	943				
sg200-18_fi	rmware		Ayuln	orability	in the u	vob				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	interfa Busine Series allow a remote user to The vu improp the par reques exploit interce reques interfa to a sp This ty known attack	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.		N/A		0-CIS-S 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

sg200-26_fir				5 Description & CVE ID						
sg200-26_fir			CVE ID : CVE-2019-1943							
	rmware						1		I	
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943				N/A		0-CIS-S 130819	
sg200-26fp_	firmware								-	
Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP			N/A		0-CIS-S 130819		
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943		
sg200-26p_	firmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SG20- 130819/571
sg200-50_fi			A uninorphility in the web		0-CIS-SG20-
URL Redirectio	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small	N/A	130819/572
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 272	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE	ID	Pat	ch	NCIIP	C ID
n to Untrusted Site ('Open Redirect')			Business 200, 300, and Series Switches softwar allow an unauthenticate remote attacker to redii user to a malicious web The vulnerability is due improper input validati the parameters of an H' request. An attacker cor exploit this vulnerabilite intercepting a user's HT request and modifying request that causes the interface to redirect the to a specific malicious U This type of vulnerabilite known as an open redin attack and is used in ph attacks that get users to unknowingly visit malite sites. CVE ID : CVE-2019-19	re could ed, rect a o page. e to ion of TTP uld cy by TTP it into a web e user JRL. ty is rect uishing o cious				
sg200-50fp	_firmware							
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the w interface of Cisco Small Business 200, 300, and Series Switches softwar allow an unauthenticat remote attacker to redi user to a malicious web The vulnerability is due improper input validati the parameters of an H' request. An attacker co exploit this vulnerabilit intercepting a user's HT request and modifying request that causes the interface to redirect the to a specific malicious U	500 re could ed, rect a o page. e to ion of TTP uld cy by FTP it into a web e user	N/A		0-CIS-S 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 273	5-6	6-7	7-8	8-9	9-10

CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	
				273						

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			This type of vulnerability is known as an open redirect attack and is used in phishin attacks that get users to unknowingly visit malicious sites.	ng			
			CVE ID : CVE-2019-1943				
sg200-50p_	firmware						
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software co allow an unauthenticated, remote attacker to redirect user to a malicious web pag The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it information request that causes the web interface to redirect the use to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishin attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	nuld a ge. of N/A N/A ng		0-CIS-S 130819	
sg300-10_fi	rmware						
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software co allow an unauthenticated, remote attacker to redirect	ould		0-CIS-S 130819	
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-	6 6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.		
cc200 10m	n finnersono		CVE ID : CVE-2019-1943		
sg300-10m URL Redirectio n to Untrusted Site ('Open Redirect')	p_nrmware 17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to	N/A	0-CIS-SG30- 130819/576
CV Scoring S					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				275						

Weakness	Publ	ish Date	CVSS	I	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
				unknov sites.	wingly v	isit mali	cious				
) : CVE-2	019.10	43				
sg300-10m	nn fir	mware					- TJ				
URL Redirectio n to Untrusted Site ('Open Redirect')		7-2019	5.8	interfa Busine Series allow a remote user to The vu improp the pan reques exploit interce reques interfa to a sp This ty known attack unknow sites.	in unaut attacke a malic: Inerabil per inpu cameters t. An att this vul	co Smal 300, and s softwa henticat ir to red ious wel ity is du t validat s of an H acker co nerabili user's H odifying uses the lirect th alicious lnerabil sed in pl t users t isit mali	l 500 re could ced, irect a b page. e to ion of TTP ould ty by TTP it into a e web e user URL. ity is rect nishing o icious	N/A		0-CIS-S 130819	
sg300-10p_	firmu	/aro		CVLIL			15				
56000 10P		ui c		Avuln	erahility	in the w	veh				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-0	7-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP			N/A		0-CIS-S 130819		
CV Scoring So (CVSS)	cale	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	Description & CVE ID	Patch	NCIIPC ID
			request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.		
sg300-10pp	Guine		CVE ID : CVE-2019-1943		
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SG30- 130819/579

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				277						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-10sfj	p_firmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SG30- 130819/580
sg300-20_fi	rmware				
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a	N/A	0-CIS-SG30- 130819/581
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 278	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943		
sg300-28_fi	rmware			I	
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SG30- 130819/582
sg300-28m	p_firmware		A 1 100 0 1 1		
URL Redirectio n to	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500	N/A	0-CIS-SG30- 130819/583
CV Scoring So (CVSS)	cale 0-1	1-2	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	NCIIF	PC ID
Untrusted Site ('Open Redirect')			Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943				
sg300-28p_	firmware						
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is	N/A		0-CIS-S 130819	
CV Scoring So	cale 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	4-5	5-6	6-7	7-8	8-9	
				280						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.		
sg300-28pp	C.		CVE ID : CVE-2019-1943		
	URL		A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP		
ORL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A	0-CIS-SG30- 130819/585
sg300-52_fi	rmwaro		CVE ID : CVE-2019-1943		
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page.	N/A	0-CIS-SG30- 130819/586
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	n NC	CIIPC ID
			The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.			
			CVE ID : CVE-2019-1943			
sg300-52m	p_firmware		A vulnerability in the web			
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious	N/A		5-SG30- 19/587
CV Scoring S	ala					

L	(CV33)				282						
	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 & CVE ID				tch	NCIIP	CID
			sites.						
			CVE ID : C	VE-2019-19	43				
sg300-52p_	firmware	_							
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	interface o Business 2 Series Swit allow an ut remote att user to a m The vulner improper i the paramo request. An exploit this interceptin request an request an request that interface to to a specifi This type o known as a attack and attacks that unknowing sites.	oility in the w f Cisco Smal 00, 300, and tches softwa nauthenticat acker to red ability is du- ability is du-	l 500 re could ced, irect a o page. e to ion of TTP ould ty by TTP it into a e web e user URL. ity is rect nishing o cious	N/A		0-CIS-S 130819	
sg500-28_fi	rmware								
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerab interface o Business 2 Series Swit allow an u remote att user to a m The vulner improper i the parame request. An	N/A		0-CIS-S 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3	-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIPC ID
			exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943			
sg500-28m	pp_firmware					
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943	N/A		0-CIS-SG50- 130819/590
sg500-28p_	firmware					
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	C ID
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	allow an remote user to The vul improp the para request exploit intercep	co Small 300, and s softwa henticat r to redi ious wel ious wel ity is due t validat s of an H acker co nerabili user's H' odifying uses the lirect the licious I linerabili sed in pl t users to isit mali	l 500 re could red, irect a o page. e to ion of TTP uld ty by TTP it into a e web e user URL. ity is rect nishing o cious	N/A		0-CIS-S 130819		
sg500-52_fi	rmware		ſ						Γ	
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web				N/A		0-CIS-S 130819	
CV Scoring So (CVSS)	cale 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	n & CVE	ID	Pa	tch	NCIIP	CID
			interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. CVE ID : CVE-2019-1943							
			CVE ID	: CVE-2	019-19	43				
crossmatch		500 dm	iwan fim							
algital_pers	ona_u.are.u_4	500_ar				11.1			[
N/A	16-07-2019	4.3	An issue was discovered in the HID Global DigitalPersona (formerly Crossmatch) U.are.U 4500 Fingerprint Reader Windows Biometric Framework driver 5.0.0.5. It has a statically coded initialization vector to encrypt a user's fingerprint image, resulting in weak encryption of that. This, in combination with retrieving an encrypted fingerprint image and encryption key (through another vulnerability), allows an attacker to obtain a user's fingerprint image. CVE ID : CVE-2019-13603			N/A		0-CR0- 130819		
Debian										
debian_linu	X									
N/A	17-07-2019	7.2	In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root			N/A		O-DEB- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is incorrect marking of a ptrace relationship as privileged, which is exploitable through (for example) Polkit's pkexec helper with PTRACE_TRACEME. NOTE: SELinux deny_ptrace might be a usable workaround in some environments. CVE ID : CVE-2019-13272		
N/A	25-07-2019	10	Exim 4.85 through 4.92 (fixed in 4.92.1) allows remote code execution as root in some unusual configurations that use the \${sort } expansion for items that can be controlled by an attacker (e.g., \$local_part or \$domain). CVE ID : CVE-2019-13917	N/A	O-DEB-DEBI- 130819/595
Dlink					
dsl-2750u_f	firmware				
Improper Authentica tion	23-07-2019	6.4	D-Link DSL-2750U 1.11 is affected by: Authentication Bypass. The impact is: denial of service and information leakage. The component is: login. CVE ID : CVE-2019-1010155	N/A	O-DLI-DSL 130819/596

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
202										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Fedoraproj	ect			<u> </u>	
fedora					
Improper Input Validation	16-07-2019	5	A vulnerability was discovered in DNS resolver of knot resolver before version 4.1.0 which allows remote attackers to downgrade DNSSEC-secure domains to DNSSEC-insecure state, opening possibility of domain hijack using attacks against insecure DNS protocol. CVE ID : CVE-2019-10191	https://ww w.knot- resolver.cz /2019-07- 10-knot- resolver- 4.1.0.html	O-FED-FEDO- 130819/597
N/A	17-07-2019	7.2	In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is incorrect marking of a ptrace relationship as privileged, which is exploitable through (for example) Polkit's pkexec helper with PTRACE_TRACEME. NOTE: SELinux deny_ptrace might be a usable workaround in some environments.	N/A	O-FED-FEDO- 130819/598

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
288										

Г

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-13272		
Improper Input Validation	17-07-2019	7.5	LibreOffice has a feature where documents can specify that pre-installed scripts can be executed on various document events such as mouse-over, etc. LibreOffice is typically also bundled with LibreLogo, a programmable turtle vector graphics script, which can be manipulated into executing arbitrary python commands. By using the document event feature to trigger LibreLogo to execute python contained within a document a malicious document a malicious document could be constructed which would execute arbitrary python commands silently without warning. In the fixed versions, LibreLogo cannot be called from a document event handler. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5. CVE ID : CVE-2019-9848	https://ww w.libreoffic e.org/abou t- us/security /advisories /CVE- 2019-9848	O-FED-FEDO- 130819/599
Informatio n Exposure	17-07-2019	4	LibreOffice has a 'stealth mode' in which only documents from locations deemed 'trusted' are allowed to retrieve remote resources. This mode is not the default mode, but can be enabled by users who want to disable LibreOffice's ability to include remote resources within a document. A flaw existed	https://ww w.libreoffic e.org/abou t- us/security /advisories /CVE- 2019-9849	O-FED-FEDO- 130819/600
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
НЗС			where bullet graphics were omitted from this protection prior to version 6.2.5. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5. CVE ID : CVE-2019-9849		
h3cloud_os					
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	19-07-2019	7.5	H3C H3Cloud OS all versions allows SQL injection via the ear/grid_event sidx parameter. CVE ID : CVE-2019-12193	N/A	0-H3C-H3CL- 130819/601
htek					
uc902_firm	ware			_	-
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	9	The Htek UC902 VoIP phone web management interface contains several buffer overflow vulnerabilities in the firmware version 2.0.4.4.46, which allow an attacker to crash the device (DoS) without authentication or execute code (authenticated as a user) to spawn a remote shell as a root user.	N/A	0-HTE-UC90- 130819/602
** •			CVE ID : CVE-2019-12325		
Huawei honor_magi	c_2_firmware				
Informatio n Exposure	17-07-2019	4.3	There is an information disclosure vulnerability on Secure Input of certain Huawei	N/A	O-HUA- HONO-
	cale 0.1				

Weakness	Publish Date	CVSS	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID	
			smartphones in Versions earlier than Tony-AL00B 9.1.0.216(C00E214R2P1). The Secure Input does not properly limit certain system privilege. An attacker tricks the user to install a malicious application and successful exploit could result in information disclosure.					130819	/603	
			CVE ID : CVE-2	2019-52	22					
linaro										
op-tee		_								
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-07-2019	7.5	Linaro/OP-TEE OP-TEE Prior to version v3.4.0 is affected by: Boundary checks. The impact is: This could lead to corruption of any memory which the TA can access. The component is: optee_os. The fixed version is: v3.4.0. CVE ID : CVE-2019-1010292			N/A		0-LIN-0 130819		
Linksys			<u> </u>			<u> </u>		<u> </u>		
re6400_firm	iware									
Improper Input Validation	17-07-2019	10	Unsanitized user input in the web interface for Linksys WiFi extender products (RE6400 and RE6300 through 1.2.04.022) allows for remote command execution. An attacker can access system OS configurations and commands that are not intended for use beyond the web UI. CVE ID : CVE-2019-11535			oads.l s.com port// /relea es/Lin %20F 0%20 00%20 00%20 mwar Relea 0Note	naws. downl inksy /sup assets asenot nksys E630 PRE64 0Fir re%20 se%2	0-LIN-F 130819		
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
				t						
re6300_firm	nware				I					
Improper Input Validation	17-07-2019	10	Unsanitized user input in the web interface for Linksys WiFi extender products (RE6400 and RE6300 through 1.2.04.022) allows for remote command execution. An attacker can access system OS configurations and commands that are not intended for use beyond the web UI. CVE ID : CVE-2019-11535	http://s3.a mazonaws. com/downl oads.linksy s.com/sup port/assets /releasenot es/Linksys %20RE630 0%20RE64 00%20Fir mware%20 Release%2 0Notes_v1. 2.05.001.tx t	0-LIN-RE63- 130819/606					
Linux										
linux_kerne	el									
Out-of- bounds Write	17-07-2019	4.6	In parse_hid_report_descriptor in drivers/input/tablet/gtco.c in the Linux kernel through 5.2.1, a malicious USB device can send an HID report that triggers an out-of-bounds write during generation of debugging messages. CVE ID : CVE-2019-13631	N/A	0-LIN-LINU- 130819/607					
N/A	19-07-2019	4.9	In the Linux kernel through 5.2.1 on the powerpc platform, when hardware transactional memory is disabled, a local user can cause a denial of service (TM Bad Thing exception and system crash) via a sigreturn() system call that sends a crafted signal frame. This affects	N/A	0-LIN-LINU- 130819/608					
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10					
(CVSS)			292							

Weakness	Publis	h Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
	arch/powerpc/kernel/signal_ 32.c and arch/powerpc/kernel/signal_ 64.c. CVE ID : CVE-2019-13648 In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace										
N/A	17-07-	·2019	7.2	_						0-LIN-L 130819	
Linuxfound	ation										
open_netwo	ork_ope	erating_	systen	1							
Improper Input Validation	22-07-	2019	7.5	The Linux Foundation ONOS 1.15.0 and ealier is affected by: Improper Input Validation. The impact is: The attacker				N/A		0-LIN-0 130819	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can remotely execute any commands by sending malicious http request to the controller. The component is: Method runJavaCompiler in YangLiveCompilerManager.jav a. The attack vector is: network connectivity.		
			CVE ID : CVE-2019-1010234		
Improper Input Validation	19-07-2019	7.5	The Linux Foundation ONOS SDN Controller 1.15 and earlier versions is affected by: Improper Input Validation. The impact is: A remote attacker can execute arbitrary commands on the controller. The component is: apps/yang/src/main/java/org /onosproject/yang/impl/Yang LiveCompilerManager.java. The attack vector is: network connectivity. The fixed version is: 1.15. CVE ID : CVE-2019-1010245	N/A	O-LIN-OPEN- 130819/611
Integer Overflow or Wraparou nd	18-07-2019	5.5	The Linux Foundation ONOS 2.0.0 and earlier is affected by: Integer Overflow. The impact is: A network administrator (or attacker) can install unintended flow rules in the switch by mistake. The component is: createFlow() and createFlows() functions in FlowWebResource.java (RESTful service). The attack vector is: network management and connectivity. CVE ID : CVE-2019-1010249	N/A	O-LIN-OPEN- 130819/612
Improper	18-07-2019	5.5	The Linux Foundation ONOS	N/A	O-LIN-OPEN-
CV Scoring Sc (CVSS)	cale 0-1	1-2	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
Input Validation			2.0.0 and earlier is affected Poor Input-validation. The impact is: A network administrator (or attacker can install unintended flow rules in the switch by mist The component is: createFlow() and createFlows() functions in FlowWebResource.java (RESTful service). The atta vector is: network management and connection CVE ID : CVE-2019-10102) v ake. uck vity.		130819/613
Improper Input Validation	18-07-2019	5.5	The Linux Foundation ONG 2.0.0 and earlier is affected Poor Input-validation. The impact is: A network administrator (or attacker can install unintended flow rules in the switch by mist The component is: applyFlowRules() and app functions in FlowRuleManager.java. Th attack vector is: network management and connecti CVE ID : CVE-2019-10102	l by:) v ake. ly() e vity.		0-LIN-OPEN- 130819/614
Paloaltonet	works					
pan-os						
Informatio n Exposure	16-07-2019	6.5	Information disclosure in I OS 7.1.23 and earlier, PAN 8.0.18 and earlier, PAN-OS 8.1.8-h4 and earlier, and P OS 9.0.2 and earlier may al for an authenticated user w read-only privileges to ext the API key of the device and/or the	-OS https://urityac AN- ries.pa llow onetw with com/H	dviso iloalt orks. iome	0-PAL-PAN 130819/615
CV Scoring So (CVSS)	cale 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 & CVE ID	Patch	NCIIPC ID
			username/password from the XML API (in PAN-OS) and possibly escalate privileges granted to them.		
			CVE ID : CVE-2019-1575		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	16-07-2019	6.5	Command injection in PAN-0S 9.0.2 and earlier may allow an authenticated attacker to gain access to a remote shell in PAN-OS, and potentially run with the escalated user?s permissions. CVE ID : CVE-2019-1576	https://sec urityadviso ries.paloalt onetworks. com/Home /Detail/15 6	O-PAL-PAN 130819/616
Improper Input Validation	19-07-2019	6.8	Remote Code Execution in PAN-OS 7.1.18 and earlier, PAN-OS 8.0.11-h1 and earlier, and PAN-OS 8.1.2 and earlier with GlobalProtect Portal or GlobalProtect Gateway Interface enabled may allow an unauthenticated remote attacker to execute arbitrary code.	N/A	O-PAL-PAN 130819/617
			CVE ID : CVE-2019-1579		
Qualcomm					
qcs404_firn	iware				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS4- 130819/618
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 296	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Ра	tch	NCIIP	C ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2235							
Improper Input Validation	25-07-2019	2.1					w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2239		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Vired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA6584, QCA9380, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD	duct- security/b ulletins	0-QUA-QCS4- 130819/620
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9206, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2241	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS4- 130819/621
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS4- 130819/622
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 299	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660		
ipq8074_fi	rmware		CVE ID : CVE-2019-2346		
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereferenceduring secure applicationtermination using specificapplication ids. in SnapdragonAuto, Snapdragon Compute,Snapdragon Connectivity,Snapdragon ConsumerElectronics Connectivity,Snapdragon Consumer IOT,Snapdragon Mobile,Snapdragon Nobile,Snapdragon WiredInfrastructure and Networkingin IPQ8074, MDM9206,MDM9607, MDM9650,MDM9655, MSM8996AU,QCA8081, QCS605, Qualcomm215, SD 410/12, SD 425, SD427, SD 430, SD 435, SD 439 /SD 429, SD 450, SD 625, SD632, SD 636, SD 650/52, SD675, SD 712 / SD 710 / SD 670,SD 730, SD 820, SD 820A, SD835, SD 8CX, SDA660,SDM439, SDM630, SDM660,Snapdragon_High_Med_2016,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-IPQ8- 130819/623

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				300						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130		
			CVE ID : CVE-2019-2236		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6574, QCA6584AU, QCA6884, QCA6584AU, QCA6884, QCA6584AU, QCA6884, QCA6584AU, QCA6584, QCA6574AU, QCA6584, QCA6584AU, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-IPQ8- 130819/624
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other	https://ww w.qualcom	0-QUA-IPQ8- 130819/625
CV Scoring So	cale				
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-6 301	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			can lea disclos Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Infrastr in IPQ8 MDM9 QCA80 215, SI SD 425 435, SI SD 425 435, SI SD 625 650/52 710 / S SD 820 850, SI SDM43 Snapdr	d to info ure in Si ragon Co ragon Co ragon Co ragon Mo ragon Mo ragon W ructure a 3074, MI 206, MD 650, MS 81, QCS 0 210/SI 650, MS 81, QCS 0 210/SI 6, SD 427 0 439 / S 5, SD 632 2, SD 670, S 6, SD 632 2, SD 671 50 670, S 6, SD 83 0 855, SI 69, SDM6 ragon_Hi 30	ormation napdrag ompute, onnective dustrial obile, nice & M ired and Net DM9150 M99067, M899664 605, Qua D 212/S 7, SD 430 SD 429, S 2, SD 636 5, SD 710 SD 730, S 35, SD 84 D 730, S 35, SD 84 D 8CX, S 530, SDM	on Auto, ity, IOT, IOT, usic, working , U, alcomm D 205,), SD SD 450, 5, SD 2 / SD SD 450, 45 / SD DA660, 4660, _2016,	m.com mpan duct- securi ulletin	y/pro ity/b		
Improper Validation of Array Index	25-07-2019	7.2	CVE ID : CVE-2019-2261 Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435,				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description 8	CVE ID	Pa	tch	NCIIP	CID
			SD 450, SD 625, SI 712 / SD 710 / SD SD 835, SD 845 / S 855, SD 8CX, SDA6 SDM630, SDM660	670, SD 820, SD 850, SD 660,				
			CVE ID : CVE-201	9-2346				
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound v triggered by a spe command supplied userspace applicat Snapdragon Auto, Consumer Electro Connectivity, Snap Consumer IOT, Sn Industrial IOT, Sn Industrial IOT, Sn Mobile, Snapdrago Infrastructure and in IPQ4019, IPQ80 IPQ8074, MDM91 MDM9206, MDM9 MDM9640, MDM9 MDM9640, MDM9 MSM8996AU, QCA QCA6574AU, QCA QCA6574AU, QCA QCA6574AU, QCA SD 210/SD 212/S 425, SD 427, SD 43 SD 450, SD 600, SI 636, SD 675, SD 7 SD 670, SD 730, SI 820A, SD 835, SD 4 SDX24	cially-crafted d by a tion. in Snapdragon apdragon apdragon on Voice & n Wired l Networking 064, 50, 607, 650, 607, 650, 6174A, 8081, 79, QCS605, D 205, SD 30, SD 435, D 205, SD 30, SD 435, D 205, SD 12 / SD 710 / D 820, SD 845 / SD 660, SDX20,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	-
qca6174a_f	irmware		CVE ID : CVE-2019-2299					
N/A	25-07-2019	2.1	While sending the surface content to Error handling is a checked results in unpredictable beh	w.qua m.con		0-QUA- 130819	•	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4	1-5 5-6	6-7	7-8	8-9	9-10

Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Nobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,security/b ulletins	
IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDM630, SDM660, SDX20, SDX24, SXR1130	
Out-of- bounds Read25-07-201910Possible out of bound read occurs while processing beaconing request due to lack of check on action frames space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Mobile,https://ww w.codeauro ra.org/secu 19/07/01/ 130819/ 0-QUA-0	-
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 Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670 SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24	bulletin	
			CVE ID : CVE-2019-2276		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA6- 130819/630
Out-of-	25-07-2019	7.5	Out of bound access when	https://ww	0-QUA-QCA6-
bounds CV Scoring Sc			reason code is extracted from	w.codeauro	130819/631
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-6 305	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
Read			the fran Snapdr Consum Consum Industr Mobile, Music i MDM92 MDM96 MSM89 QCA65 QCA93 425, SE SD 450 665, SE SD 670 820A, S 850, SE SDM66	data with me lengt agon Au ner Elect ctivity, Si ner IOT, rial IOT, Si n MDM9 206, MD 206, SD 206, SD	th in ito, Snap tronics napdrag Snapdra sagon Vo 9150, M9607, M9650, QCA6174 (CA9377 405, QCS 0 430, SI 5, SD 636 0 712 / S 0, SD 820 SD 845 / DA660, S 0, SDX24	odragon gon agon agon oice & 4A, 5605, SD 0 435, 5, SD 5D 710 / 5D 710 / 0, SD 7 SD 5DM630, 4	rity- bullet	a- ity-		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	CVE ID : CVE-2019-2305 Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA65, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	•
CV Scoring So										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2307		
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2309	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA6- 130819/633
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA6- 130819/634
(CVSS)	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	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
				Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312 While sending the rendered							
qca6564_fir	mwar	e									
N/A	25-07	7-2019	2.1	surface Error h checke unpred Snapdr Comput Connec Consur Industr IoT, Sn Snapdr Snapdr Infrast in IPQ4 IPQ807 MDM9 MDM9 MSM89 QCA65 QCA65 QCA65 QCA65	e conten aandling d results lictable l ragon Au te, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, ragon Vo ragon Vo ragon W ructure 2019, IP(74, MDM 206, MD 640, MD 640, MD 640, MD 640, QCA 74AU, Q 84AU, Q	t to the s is not p s in an behaviou ito, Snap dragon napdrag tronics napdrag snapdrag on Mobil bice & Mi ired and Netv Q8064, 19150, M9607, M9607, QCA6174 6574, QCA6584 QCA6584 QCA6584	screen, roperly ur in odragon gon agon agon e, usic, working 4A,	w.qua m.con mpan duct- secur ulletin	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				308						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240		
qca6574_fir	mware				
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Vired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA9379, QCA9531, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCA6- 130819/636
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 3 09	6-7 7-8	8-9 9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				309						

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIF	PC ID
			670, SI SD 835 855, SI SDM63	0 730, SI , SD 845 0 8CX, SI	660, SDX	D 820A, 50, SD				
			CVE ID	: CVE-2	019-22	40				
qca6574au	_firmware									
N/A	25-07-2019	2.1	surface Error h checke unpred Snapdr Compu Consur Consur Industr IoT, Sn Snapdr Snapdr Infrastr in IPQ4 IPQ807 MDM99 MDM99 MDM99 MDM97 MDM97 MDM97 MDM97 MDM97 MDM97 Snapdr Infrastr in IPQ4 IPQ807 MDM97 MDM97 MDM97 MDM97 MDM97 MDM97 MDM97 Snapdr Infrastr in IPQ4 IPQ807 MDM97 SD 210 425, SI SD 675 670, SI	e contem aandling d results lictable l ragon Au te, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, apdrago ragon Vo ragon W ructure 019, IPO 74, MDM 206, MD 640, SI 77, QCA 80, QCA 02, QCS /SD 212 0 600, SI , SD 712 0 730, SI	behavior ito, Snap dragon napdrag tronics napdrag Snapdr S	screen, roperly ur in odragon gon agon agon e, usic, working 4A, , , CA9531, CA9531, CA9980, 5605, 5, SD D 636, 0 / SD D 636, 0 / SD	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4 310	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ſ	Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			SDM63	D 8CX, SI 80, SDM6 , SXR113	60, SDX	20,				
			CVE ID) : CVE-2	019-22	40				
Out-of- bounds Read	25-07-2019	10	occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Woice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Dat	e CVSS	Description & CVE ID	Patch	NCIIPC ID
			450, SD 625, SD 632, SD 636 SD 665, SD 675, SD 712 / SI 710 / SD 670, SD 730, SD 82 SD 820A, SD 835, SD 845 / S 850, SD 855, SDA660, SDM4 SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_201	D 20, SD 139,	
			CVE ID : CVE-2019-2279		
Out-of- bounds Write	22-07-2019	9 7.5	Improper validation for inp received from firmware can lead to an out of bound writ issue in video driver. in Snapdragon Auto, Snapdrag Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearabl in MDM9150, MDM9206, MDM9607, MDM9640, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 200 SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 45 SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 71 SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM4 SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287	a https://ww gon https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin 10 /	0-QUA-QCA6- 130819/640
Improper			Out of bound access can occ	1 , ,	
Restriction of Operations within the	22-07-2019	9 4.6	due to buffer copy without checking size of input receiv from WLAN firmware in Snapdragon Auto, Snapdrag	rity-	0-QUA-QCA6- 130819/641

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	C ID
Bounds of a Memory Buffer			Industr Mobile, Music i MDM96 QCA65 SD 210 425, SE SD 450 665, SE SD 730 845 / S SDM63 SDX24	ner IOT, rial IOT, S , Snapdra n MDM9 650, MSN 74AU, Q0 /SD 212 0 427, SD 0 427, SD 0 427, SD 0 712 / S 0 712 / S 0 712 / S 0 850, S 50, SDM6	Snapdra agon Vo 150, M8996A CS405, (/SD 205 0 430, SI , SD 636 D 710 / A, SD 83 D 855, S 60, SDX	agon ice & U, QCS605, 5, SD D 435, 5, SD SD 670, 35, SD SDA660, 20,	19/06 june-2 code- auror secur bullet	a- ity-		
Integer Overflow or Wraparou nd	25-07-2019	4.6	trigger comma userspa Snapdr Consum Consum Industr Mobile, Music, S Infrastr in IPQ4 IPQ807 MDM92 MDM92 MDM94 MDM94 QCA65 QCA93 SD 210 425, SE SD 450 636, SE SD 670 820A, S	of-bound ed by a synd suppl ace appli agon Aut ner Elect ctivity, Sr ner IOT, cial IOT, S , Snapdrag ructure a 206, MDI 206, SD 74AU, QC 77, QCAS 2427, SD 2427, SD 50 835, SD 50 835, SD	pecially lied by a cation. : to, Snap cronics napdrag Snapdra Snapdra agon Vo gon Wir and Netw 28064, 9150, M9607, M9650, 2606174 CA8081 9379, Q0 /SD 205 9430, SI , SD 625 9712 / S , SD 820 50 845 /	-crafted a in odragon agon agon ice & red working 4A, , CS605, 5, SD 0 435, 5, SD 0 435, 5, SD 5D 710 / 0, SD	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So	cale 0-1	1-2	2-3	,	-,-	5-6	6-7	7-8	8-9	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 CVE ID : CVE-2019-2299		
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA6- 130819/643
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA6- 130819/644
CV Scoring So (CVSS)	cale 0-1	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	NCIII	PC ID
			QCA6174A, QCA6574A QCA9377, QCA9379, QC QCS605, SD 210/SD 212 205, SD 425, SD 427, SD SD 435, SD 450, SD 600 625, SD 636, SD 665, SD SD 712 / SD 710 / SD 6 730, SD 820, SD 820A, S SD 845 / SD 850, SD 85 SDM630, SDM660, SDX2 SDX24	CS405, 2/SD 0 430, , SD 0 675, 70, SD SD 835, 5, 20,				
			CVE ID : CVE-2019-23					
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated from firmware in cache integer overflow may of since data length receiv exceed real data length. Snapdragon Auto, Snap Consumer Electronics Connectivity, Snapdrage Consumer IOT, Snapdra Industrial IOT, Snapdra Mobile, Snapdragon Voi Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174 QCA6574AU, QCA6174 QCA6574AU, QCA6174 QCA6574AU, QCA9377, QCA9379, SD 210/SD 2 205, SD 425, SD 625, SD SD 712 / SD 710 / SD 6 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-23	An ccur red may . in dragon on agon gon ice & AA, 12/SD 0 636, 70, SD	https: w.cod ra.org rity- bullet 19/07 july-2 code- aurora securi bullet	eauro /secu in/20 7/01/ 019- a- ity-	0-QUA- 130819	
Improper Restriction of Operations	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of		https:/ w.cod ra.org rity-	eauro	0-QUA- 130819	
within the Bounds of			data buffer received in Snapdragon Auto, Snapdragon		bullet 19/07			
CV Scoring So	cale				-			0.40
(CVSS)	0-1	1-2	2-3 3-4 4-5 315	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	july-2019- code- aurora- security- bulletin	
qca6584_fii	rmware		CVE ID . CVE-2019-2312		
N/A CV Scoring S	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCA6- 130819/647

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				316						

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	D	Pat	tch	NCIIP	CID
			QCA65 QCA93 QCA93 QCA98 QCN55 SD 210 425, SI SD 675 670, SI SD 835 855, SI SDM63	64, QCA 74AU, Q 84AU, Q 77, QCA 80, QCA 02, QCS /SD 212 0 600, SE , SD 712 0 730, SE , SD 845 0 8CX, SE 0, SDM6 , SXR113	CA6584 CA8081 9379, Q(9886, Q(404, QCS /SD 205 /SD 205 /SD 71 0 820, SI /SD 85 0A660, 560, SDX	, CA9531, CA9980, 5605, 5, SD 0636, 0636, 0/SD 0820A, 0, SD				
			CVE ID	: CVE-2	019-22	40				
qca6584au	firmware									
N/A	25-07-2019	2.1	surface Error h checke unpred Snapdr Compu Connec Consur Industr IoT, Sn Snapdr Snapdr Infrastr in IPQ4 IPQ807 MDM97 MDM97 MSM89 QCA65 QCA65	sending f content andling d results lictable b ragon Au te, Snap ctivity, Sn ner Elec ctivity, Sn ner IOT, rial IOT, ragon Vo ragon Vo ragon Vo ragon Wi ructure a c019, IPC 74, MDM 206, MD 206, MD	to the s is not pro- s in an behaviou ito, Snap dragon napdrag snapdrag Snapdrag Snapdra Snapdrag Snapdra n Mobile ice & Mu ired and Netw 28064, 9150, M9607, M9650, QCA6174 6574, CA6584	creen, operly Ir in dragon on on agon gon e, Isic, working	https: w.qua m.con duct- securi ulletin	n/co y/pro ty/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9
			317					

Weakness	Publish Date	CVSS	Description & CVE	ID	Patch	NCIIP	C ID
			QCA9377, QCA9379, Q QCA9880, QCA9886, Q QCN5502, QCS404, QC SD 210/SD 212/SD 203 425, SD 600, SD 625, SI SD 675, SD 712 / SD 71 670, SD 730, SD 820, SI SD 835, SD 845 / SD 85 855, SD 8CX, SDA660, SDM630, SDM660, SDX SDX24, SXR1130 CVE ID : CVE-2019-22	CA9980, S605, 5, SD D 636, L0 / SD D 820A, S0, SD			
qca9377_fir	mware						
N/A	25-07-2019	2.1	While sending the rend surface content to the s Error handling is not p checked results in an unpredictable behaviou Snapdragon Auto, Snap Compute, Snapdragon Connectivity, Snapdrag Consumer Electronics Connectivity, Snapdrag Consumer IOT, Snapdra Industrial IOT, Snapdra IoT, Snapdragon Mobil Snapdragon Voice & M Snapdragon Wired Infrastructure and Nett in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9650, MSM8996AU, QCA6174 QCA6564, QCA6574, QCA6574AU, QCA6584 QCA6584AU, QCA6384 QCA6584AU, QCA8081 QCA9377, QCA9379, QU QCA9880, QCA9886, QU QCN5502, QCS404, QC3	screen, roperly ur in odragon gon agon http agon m.c usic, mpa duc working secu ulle 4A, , , , , , , , , , , , , , , , , , ,	os://ww ualcom om/co any/pro t- urity/b etins	0-QUA-(130819	-

2-3	3-4	4-5	
	318		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130		
			CVE ID : CVE-2019-2240		
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA9- 130819/650
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA9- 130819/651
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24		
Out-of- bounds Read	25-07-2019	7.5	CVE ID : CVE-2019-2299 Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA9- 130819/652

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				320						

Weakness	Publish Date	CVSS	Description & CVE ID				Ра	tch	NCIIF	PC ID
			CVE ID) : CVE-2	2019-23	05				
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	due to calcula 802.11 configu Auto, S Electro Snapdu Snapdu Snapdu Snapdu Snapdu MDM9 MDM9 QCA61 QCA93 QCS60 205, SI SD 435 625, SI SD 712 730, SI SD 845 SDM63 SDX24	lata leng agemen n Snapd gon Cons nnectivit onsumer dustrial	n before th in t ragon sumer ty, IOT, IOT, usic in U, U, CS405, 2/SD D 430, D 430, D 675, 570, SD SD 835, 55, 520,	w.cod ra.org rity- bullet	a- ity-	0-QUA-QCA9- 130819/653		
Out-of- bounds Read	25-07-2019	7.5	from fi integer since d exceed Snapdr Consur Consur Indust Mobile	a length ito, Snap tronics napdrag Snapdra Snapdra ragon Vo	e, An occur ved may . in odragon gon agon agon oice &	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	v	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	CID
			MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20							
			CVE ID	: CVE-2	019-23	09				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2309 When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	-
qca9379_fir	mware									
N/A	25-07-2019	2.1	surface Error h checkee unpred	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon			w.qua m.con	n/co y/pro	0-QUA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	CID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130				ulletin	15		
Out-of- bounds Read	25-07-2019	10	occurs beacon of chec receive space in Snapdr Electro Snapdr Snapdr	bound r ocessin iest due ion fram user con ragon A nagon A nsumer nectivit nsumer obile, ice & M	g to lack es trolled uto, y, IOT,	w.cod ra.org rity- bullet	a-	0-QUA- 130819	•	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24	bulletin	
			CVE ID : CVE-2019-2276		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA9- 130819/658
Out-of- bounds	25-07-2019	7.5	Out of bound access when reason code is extracted from	https://ww w.codeauro	0-QUA-QCA9-
Read			frame data without validating	ra.org/secu	130819/659
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	PC ID
			Snapdr Consur Consur Industr Mobile Music i MDM9 MSM89 QCA65 QCA93 425, SI SD 450 665, SI SD 670 820A, S 850, SI SDM66	, SD 730 SD 835, S	to, Snap tronics napdrag Snapdra agon Vo 0150, M9607, M9650, QCA6174 CA9377 405, QCS 0 430, SI , SD 636 0 712 / S , SD 820 SD 845 / 0A660, S 0, SDX24	agon agon ice & 4A, , 5605, SD 0 435, 5, SD 5D 710 / 0, SD ' SD 5DM630, 4	rity- bullet 19/07 july-2 code- auror securi bullet	019- a- ity-		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	due to calcula 802.11 configu Auto, S Electro Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 QCA61 QCA93 QCS60 205, SI	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD		w.cod	7/01/ 019- a- ity-	0-QUA- 130819	-	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 325	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2307		
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2309	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA9- 130819/661
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA9- 130819/662
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

N/AZ5-07-2019Z.IXI A CASTA, CCASTAU, CCAST	Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
N/A25-07-20192.1While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9650, MDM9640, MDM9650, MDM9640, MDM9650, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6584AU, QCA6584, QCA6584AU, QCA6057, MDM9640, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QC6654, QCA552, QCS404, QC6654, QCA6554, QCA6554, QCA6584AU, QCA6174A, QCA6584AU, QCA6574, QCA6584AU, QCA6574, QCA5886, QCA9980, QCN5502, QCS404, QC5605,A 12A 1556677889101				QCA61 QCA93 QCS60 205, SI SD 435 625, SI SD 712 730, SI SD 845 SDM63	74A, QC 77, QCA 5, SD 21 0 425, SI 5, SD 450 0 636, SI 2 / SD 71 0 820, SI 5 / SD 85 30, SDM6	A6574A 9379, Q 0/SD 21 0 427, SI 0, SD 600 0 665, SI 0 / SD 6 0 820A, S 0, SD 85 660, SDX					
N/A25-07-20192.1surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM950, MDM9206, MDM9607, MDM9266, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6564, QCA9880, QCA9886, QCA9980, QCM9377, QCA9379, QCA9531, QCA9380, QCA9886, QCA9980, QCN5502, QCS404, QCS605,outputoutputoutputoutputCV Scoring Scale0.11/22/33/44/55/66/77/88/98/10	qca9531_fii	rmware									
			2.1	surface Error h checke unprec Snapdn Compu Consur Consur Industr IoT, Sn Snapdn Snapdn Infrast in IPQ4 IPQ807 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MSM89 QCA65 QCA65 QCA65 QCA65	e content handling d results dictable l ragon Au ite, Snap ctivity, Si ner Elec ctivity, Si ner IOT, rial IOT, apdrago ragon Vo ragon Vo ragon Wi ructure a 4019, IPO 74, MDM 206, MD 640, MD 640, MD 996AU, Q 64, QCA 74AU, Q 84AU, Q 84AU, Q	to the s is not p s in an behaviou ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra Snapdra Snapdra (Snapdra Snapdra Snapdra Snapdra (Snapdra Snapdra	AA, CA9531, CA9580,	w.qua m.con mpan duct- secur	llcom n/co y/pro ity/b	-	-
	CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

2-3	3-4	4-5	5
	327		

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			425, SI SD 675 670, SI SD 835 855, SI SDM63	/SD 212 0 600, SD 5, SD 712 0 730, SD 6, SD 845 0 8CX, SD 80, SDM6 , SXR113) 625, SI / SD 71) 820, SI / SD 85) A660,) 60, SDX	D 636, .0 / SD D 820A, 50, SD				
			CVE ID	: CVE-2	019-22	40				
Use After Free	25-07-2019	4.6	happer diag dr free iss Snapdr Snapdr Snapdr Snapdr Snapdr Infrastr in IPQ4 MDM99 MDM99 QCA95 210/SI SD 427 450, SI 650/52 670, SI SD 845 SDX20, Snapdr	to freed while re- iver due agon Co- agon Co- agon Co- agon Mo- agon Mo- agon Wi ructure a 019, IPC 206, MD- 206, MD- 640, MD- 64	eading f to use a apdrago nnectivi nsumer dustrial obile, earables red and Netv (8064, M9607, M9650, SM8996 9980, SI 0 205, S , SD 435 0 636, SI 2 / SD 7 0 820A, S 0 820A, S 0, SDM6 gh_Med	From after on Auto, ity, IOT, IOT, S, working 5AU, D 425, 5, SD D 10 / SD SD 835, 560, _2016	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	-
qca9880_fir	rmware									
N/A	25-07-2019	2.1	surface Error h checke	sending t e content andling d results lictable b	to the s is not p in an	screen, roperly	w.qua m.con		0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6564, QCA6574, QCA6584AU, QCA8081, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240	security/b ulletins	
qca9886_fin	rmware				
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCA9- 130819/666
CV Scoring S (CVSS)	cale 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	Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
				Description & CVE IDConsumer ElectronicsConnectivity, SnapdragonConsumer IOT, SnapdragonIndustrial IOT, SnapdragonIoT, Snapdragon Mobile,Snapdragon Voice & Music,Snapdragon WiredInfrastructure and Networkingin IPQ4019, IPQ8064,IPQ8074, MDM9150,MDM9206, MDM9607,MDM9640, MDM9650,MSM8996AU, QCA6174A,QCA6564, QCA6574,QCA6584AU, QCA6584,QCA6584AU, QCA6881,QCA9377, QCA9379, QCA9531,QCA9880, QCA9886, QCA9880,QCN5502, QCS404, QCS605,SD 210/SD 212/SD 205, SD425, SD 600, SD 625, SD 636,SD 675, SD 712 / SD 710 / SD670, SD 730, SD 820, SD 820A,SD 835, SD 845 / SD 850, SD855, SD 8CX, SDA660,SDM630, SDM660, SDX20,SDX24, SXR1130CVE ID : CVE-2019-2240While sending the renderedsurface content to the screen,Error handling is not properlychecked results in anunpredictable behaviour inSnapdragon Auto, SnapdragonCompute, SnapdragonConnectivity, SnapdragonConnectivity, SnapdragonConnectivity, SnapdragonConnectivity, SnapdragonConsumer ElectronicsConnectivity, Snapdragon							
qca9980_fir	mware										
N/A	25-07-2	019	2.1	surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon			w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	•	
CV Scoring So (CVSS)	cale (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	on & CVE	ID	Pa	tch	NCIIF	PC ID
			Industri IoT, Sn Snapdr Snapdr Infrastri in IPQ4 IPQ807 MDM99 MDM99 MSM89 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 SD 210 425, SI SD 210 425, SI SD 675 670, SI SD 835 855, SI SDM63 SDX24, CVE ID							
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	-
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA9- 130819/669
qcn5502_fii	rmware				
N/A	25-07-2019	2.1	 While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer Electronics Consumer IOT, Snapdragon 	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCN5- 130819/670
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130		
			CVE ID : CVE-2019-2240		
sd_665_firm	iware				
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/671
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/672
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon	https://ww w.qualcom m.com/co mpany/pro	0-QUA-SD_6- 130819/673
CV Scoring So (CVSS)	cale 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	n & CVE	ID	Pa	tch	NCIIP	CID
			Auto, Sr Snapdra Snapdra Snapdra Mobile, Music, S in MDM MDM96 MDM96 MDM96 MDM96 MDM96 MDM96 MSM89 Qualcor 212/SD SD 430, 429, SD 415, SD SD 650,	pute, IOT, IOT, Iragon ice & arables 06, 4, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7,	duct- secur: ulletin	• •				
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring Sc	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	

Weakness	Publish Date	CVSS	•			tch	NCIIF	PC ID
			SD 425, SD 427, SD 435, SD 439 / SD 4 SD 625, SD 632, SD 665, SD 712 / SD 7 SD 730, SD 820A, S 845 / SD 850, SD 8 SDM439, SDM630, SDX20, SDX24, Snapdragon_High_I SXR1130	29, SD 450, 636, SD 10 / SD 670, D 835, SD 55, SDM660, Med_2016,				
			CVE ID : CVE-2019					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer ove processing the high process action fram improper buffer len validation in Snapd Snapdragon Compu Snapdragon Compu Snapdragon Indust Snapdragon Mobile Snapdragon Voice & MDM9150, MDM96 MSM8996AU, QCS4 QCS605, SD 625, SI 665, SD 712 / SD 7 SD 730, SD 820, SD 835, SD 845 / SD 8 SDA660, SDM630, S SDX20, SDX24, SXR CVE ID : CVE-2019	-	in/20 5/03/ 2019- a- ity-	0-QUA- 130819	—	
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault v playing h265 video denial of service iss Snapdragon Auto, S Compute, Snapdrag Connectivity, Snap Consumer IOT, Sna Industrial IOT, Snap Mobile, Snapdragon	https: w.qua m.con mpan duct- securi ulletir	n/co y/pro ty/b	0-QUA- 130819		
CV Scoring S	cale 0-1	1-2	2-3 3-4 4-	5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273		
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/677
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code-	0-QUA-SD_6- 130819/678
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 337	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID		Pat	ch	NCIIF	PC ID
			Snapdragon Voice MSM8996AU, QCS QCS605, SD 210/2 205, SD 425, SD 4 SD 435, SD 450, S 636, SD 665, SD 6 SD 710 / SD 670, 820A, SD 835, SD 850, SD 855, SDA SDM660, SDX24 CVE ID : CVE-201	aurora securi bulleti	ty-			
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279		https:/ w.code ra.org rity- bulleti 19/06 june-2 code- aurora securi bulleti	eauro /secu in/20 5/03/ 2019- a- ty-	0-QUA- 130819	
Improper Restriction of Operations	25-07-2019	4.6	An unauthenticat image can be load memory and subs cause execution o	https://ww w.qualcom m.com/co mpany/pro		v.qualcom 0-QUA-SD_6 n.com/co 130819/680		
CV Scoring So	cale 0-1	1-2	2-3 3-4	2-3 3-4 4-5 5-6		7-8	8-9	9-10

Weakness	Publish Date	CVSS	•				Pa	tch	NCIIF	PC ID
within the Bounds of a Memory Buffer			Snapdr Snapdr Snapdr Snapdr QCS405 665, SD SD 670 835, SD SD 8CX SDM66	n Snapdr ragon Co ragon Co ragon Ind ragon Wo 5, QCS60 0 675, SE , SD 730 0 845 / S 5, SDA66 0, SDX2 : CVE-2	nnectivi nsumer dustrial obile, ice & Mi 05, SD 63 0, SD 820 50 850, S 0, SDM6 4, SXR12	ity, IOT, IOT, asic in 36, SD 5D 710 / 0, SD 5D 855, 30, 130	duct- securi ulletin			
NULL Pointer Dereferenc e	25-07-2019	7.8	happen with wi Snapdr Compu Consum Industr IoT, Sna Snapdr MDM92 MDM92 MSM89 QCS403 215, SE SD 425 435, SE SD 425 435, SE SD 600 625, SE SD 675 670, SE SD 835 855, SE SDM63	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016		w.qua m.con	n/co y/pro ity/b	0-QUA- 130819		
Improper	25-07-2019	2.1	Out of l	bound re	ead and		https:	//ww	O-QUA-	SD_6-
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4 339	4-5	5-6	6-7	7-8	8-9	9-10

Restriction of Operations within the Bounds of a Memoryinformation disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Noice & Music, Snapdragon Voice & Music, Snapdragon, Jigh, Med_2016, SXR1130Uther Mathematical State Music, Snapdragon Compute, Snapdragon Compute, Snapdragon Nobile, Snapdragon Music, Snapdragon MusanablesUther Music, Snapdragon Music, Snapdragon Music, Snapdragon Music, Snapdragon MusanablesUther Music, Snapdragon Music, Snapdra	Weakness	Publish Date	CVSS	De	escriptio	n & CVE	ID	Pa	tch	NCIIP	CID
Out-of- bounds Write22-07-20197.57.57.57.50.111111000000000000000000000000000000	of Operations within the Bounds of a Memory			informat firmwar checking structur a kernel Auto, Sn Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra SD 427, 3 439 / SD SD 632, 3 675, SD SD 730, 3 SD 8CX, 3 SCX 8 SD 8 SCX 8 SD 8 SCX 7 SCX 8 SD 8 SCX 8 SCX 8 SCX 8 SD 8 SCX 7 SCX 8 SD 8 SCX 7 SCX 8 SD 8 SCX 7 SCX 7	tion dis e due te g of an e e that c driver apdrag gon Co gon Co gon Co gon Mc gon We gon We OW, M Qualco 212/SI SD 430 O 429, S SD 636 712 / S SD 636 712 / S SD 820 845 / S SDA66 0, SDM6 gon_Hi O	cclosure o insuffi embedd can be se in Snape on Com nnectivi nsumer dustrial obile, ice & Mu earables SM8996 omm 21 O 205, SI , SD 435 G 450, S G 450, S G 450, S G 710 / , SD 820 G 850, S 0, SDM4 60, gh_Med	in cient ed ent from dragon pute, ty, IOT, IOT, ISIC, in 5AU, 5, SD 50 425, 5, SD 50 425, 5, SD 50 625, 5, SD 5D 670, A, SD 5D 855, 39, _2016,	m.com mpan duct- secur	n/co y/pro ity/b	130819	/682
in MDM9150, MDM9206, aurora- MDM9607, MDM9640, security- MDM9650, MSM8909W, bulletin MSM8996AU, QCA6574AU, QCS405, Qualcomm	bounds	22-07-2019	7.5	received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU,			w.cod ra.org rity- bullet 19/06 june-2 code- auror secur	leauro g/secu cin/20 6/03/ 2019- a- ity-			
CV Scoring Scale	-	cale 0-1	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/684
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-	0-QUA-SD_6- 130819/685
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 341	6-7 7-8	8-9 9-10

			Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650,	security- bulletin	
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, S 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM63 SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305	/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	5-07-2019	4.6	Improper casting of structure while handling the buffer lead to out of bound read in displa in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearable in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450 SD 615/16/SD 415, SD 625, S 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SE 730, SD 820, SD 820A, SD 835 SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/686
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	•					tch	NCIIP	CID
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	due to l calcula 802.11 configu Auto, S Electro Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 QCA61 QCA61 QCA61 QCA63 QCS60 205, SE SD 435 625, SE SD 712 730, SE SD 712 730, SE SD 845 SDM63 SDX24	e intege lack of v tion of d Rx man uration in napdrag nics Cor agon Co agon Inc agon Mo 50, MD 607, MD 607, MD 650, MSI 74A, QCA 5, SD 210 0 425, SE , SD 210 0 425, SE , SD 450 0 636, SE / SD 71 0 820, SE 0 820, SE 0, SDM6	alidation ata leng agemen n Snapd on Cons inectivit nsumer dustrial obile, ice & Mi M9206, M9640, M9996A M9574A 9379, Q0 0/SD 21 0 427, SI 0 427, SI 0 427, SI 0 665, SI 0 665, SI 0 820A, SD 0 820A, SD 0 820A, SD	n before th in t ragon sumer y, IOT, IOT, usic in U, U, CS405, 2/SD O 430, 0, SD O 675, 70, SD SD 835, 55, 20,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			SD 439 625, SE SD 675 670, SE SD 845 SDA66 SDM66	9 427, SE / SD 42 0 632, SE , SD 712 0 730, SE / SD 85 0, SDM4 0, SDX2	9, SD 45) 636, SI / SD 71) 820A, S 0, SD 85 39, SDM 0, SDX24	60, SD D 665, 0 / SD SD 835, 55, 630, 4				
			CVE ID	: CVE-2	019-23	08				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312				w.cod ra.org rity-	019- a- ity-	0-QUA- 130819	
qcs405_firn	nware									
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon				https://ww w.qualcom m.com/co mpany/pro duct- security/b		0-QUA- 130819	•
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS						tch	NCIIP	CID
			Industr IoT, Sn Snapdr Snapdr MDM9 MDM9 MSM89 QCS409 215, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63	ulletin	ns					
			A race	: CVE-2 conditio	n occurs					
Use After Free	22-07-2019	6.9	can lea conditi Snapdr Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 QCS40 215, SI SD 425 435, SI SD 625 665, SI SD 730 845 / S	ompute, onsumer dustrial obile, nice & M earables M9206, M9640, M9640, M8909V 05, Quale 0 212/S 7, SD 430 50 429, S 50 429, S 50 710 / 0A, SD 83	ree on Auto, IOT, IOT, usic, s in V, comm D 205, 0, SD SD 450, 5, SD SD 670, 35, SD	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	•	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2260		
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-QCS4- 130819/692
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-QCS4- 130819/693

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				346						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2269		
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCS4- 130819/694
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-QCS4- 130819/695
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-QCS4- 130819/696
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS4- 130819/697

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				348						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX24, SXR1130		
			CVE ID : CVE-2019-2281		
NULL Pointer Dereferenc e	Pointer Dereferenc 25-07-2019 7.8		Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS4- 130819/698
			CVE ID : CVE-2019-2334 Firmware is getting into loop		
Improper Validation of Array Index	25-07-2019	7.2	of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS4- 130819/699
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660		
			CVE ID : CVE-2019-2346		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-QCS4- 130819/700
Improper Restriction of Operations within the Bounds of	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/	0-QUA-QCS4- 130819/701
CV Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	june-2019- code- aurora- security- bulletin	
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2293	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCS4- 130819/702
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS4- 130819/703
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID		Pa	tch	NCIIF	PC ID		
			MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298							
Out-of- bounds Read	25-07-2019	7.5	reason frame of the fran Snapdr Consum Consum Industr Mobile, Music i MDM92 MDM96 MSM89 QCA65 QCA93 425, SE SD 450 665, SE SD 670 820A, S 850, SE SDM66	CVE ID : CVE-2019-2298 Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377,		w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	-	
Improper Restriction of Operations within the	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity,				w.cod ra.org rity-	//ww eauro g/secu in/20	0-QUA- 130819	•
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 352	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Ра	tch	NCIIP	C ID
Bounds of a Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20				19/02 july-2 code- auror secur bullet	a- ity-		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possibl due to calcula 802.11 configu Auto, S Electro Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 MDM9 QCA61 QCA63 QCS60 205, SI SD 435	CVE ID : CVE-2019-2306 Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675,			w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2307		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCS4- 130819/707
			When handling the vendor	https://ww	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCS4- 130819/708
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312		
mdm9615_1	firmware				
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MDM9- 130819/709
CV Scoring S					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				355						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2254		
mdm9625_1	firmware				
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/710
qca8081_fir	mware	https://			
NULL Pointer Dereferenc	25-07-2019	2.1	Null pointer dereference during secure application termination using specific	https://ww w.qualcom m.com/co	0-QUA-QCA8- 130819/711
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
e			application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236	mpany/pro duct- security/b ulletins			
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCA8- 130819/712		
1							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450,		0-0UA-0CA8-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130				
			CVE ID : CVE-2019-2261				
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCA8- 130819/714		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCA8- 130819/715		
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 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 IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24			
sd_730_firm	wara		CVE ID : CVE-2019-2299			
3u_730_1111			Null pointer dereference			
NULL Pointer Dereferenc e	Pointer Dereferenc 25-07-2019 2.1		during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_7- 130819/716	

(CVSS)	0-1	1-2	2-3	3-4 360	4-5	5-6	6-7	/-8	8-9	9-10
CV Scoring Scale	0.1	1 2	n n	2.4	4 5	ГС	67	7.0	<u>ه م</u>	0.10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2236		
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/717
			Lack of check of data type can		
Out-of- bounds Read	25-07-2019	4.6	lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/718
CV Scoring So (CVSS)	cale 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	on & CVE	ID	Pa	tch	NCIIP	C ID
				MDM9 210/SI 410/12	607, MD 655, QC D 212/S 2, SD 67 SD 670, S 30						
				CVE ID) : CVE-2	2019-22	38				
Improper Input Validation	25-07-2	2019	2.1	layout Corrup Denial Snapdu Compu Connee Consur Indust Mobile Music, Infrast in MDM MDM9 MDM9 MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52 710 / S SD 820 850, SI SDM43 SDX20 Snapdu SXR11	which c of Servi agon Au agon Au ate, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, , Snapdra ructure 49150, I 607, MD 640, MD 655, MS 4, QCS60 0 210/S 0 30 4 0 4 0 4 0 4 0 4 0 4 0 4 0 4 0 4 0 4	ato, Snap odragon napdrag ctronics napdrag Snapdra Snapdra agon Vo agon Win and Net MDM920 M96351 M96350, M99650, M99650, M8996A D5, Qual D 212/S 425, SD 0 439 / S 5, SD 71 SD 730, S 35, SD 84 DA660, 630, SDN	to SUI to odragon gon agon agon oice & red working 06, M, U, comm D 205, 427, SD SD 429, 415, SD SD 429, 415, SD D 2 / SD SD 820, 45 / SD 4660, _2016,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	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	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6584AU, QCA6174A, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/720
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading	https://ww w.qualcom m.com/co mpany/pro duct-	0-QUA-SD_7- 130819/721
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 3 63	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	Ра	tch	NCIIP	C ID	
			in Snap Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Infrast in MDM MDM9 QCS40 212/SI 636, SI SD 670 820A, S 850, SI SDM63 SXR113	itended S odragon Co ragon Co ragon Co ragon Co ragon Co ragon Mo ragon Mo ragon Mo ragon Mi ructure a 49150, M 607, MD 655, MS 4, QCS60 0 205, SI 0 675, SI 0 675, SI 0 675, SI 0 835, SI 0 835, SI 60, SDM6 30 0 : CVE-2	Auto, impute, innectivit insumer dustrial obile, ired and Netw ADM920 M9650, M8996A 05, SD 22 0 410/1 0 712 / S 0, SD 820 SD 845 / 0 8CX, SI 560, SDX	secur ulletin	• •			
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660		
			CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/723
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/724
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 365	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/725
CV Scoring So		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/726
Improper Restriction of Operations	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length	https://ww w.codeauro ra.org/secu rity-	0-QUA-SD_7- 130819/727
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 3 67	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269	bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_7- 130819/728
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack	https://ww w.codeauro ra.org/secu	O-QUA-SD_7- 130819/729
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 368	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID		Pat	ch	NCIIP	CID	
			of check on act received from t space in Snapd Snapdragon Co Electronics Con Snapdragon Mo Snapdragon Mo Snapdragon Mo Snapdragon Vo MDM9607, MS QCA6174A, QC QCA9377, QCA QCS605, SD 63 675, SD 712 / S SD 730, SD 820 850, SD 855, SI SDM660, SDX2 CVE ID : CVE-2	rity- bulleti 19/07 july-2 code- aurora securi bulleti	/01/ 019- a- ty-				
Out-of- bounds Read	22-07-2019	4.6	CVE ID : CVE-2019-2276 Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 /		https:, w.cod ra.org rity- bulleti 19/06 june-2 code- aurora securi bulleti	eauro /secu in/20 /03/ 019- a- ty-	0-QUA- 130819		
Improper Restriction of Operations	22-07-2019	7.5	Shared memor with invalid da to access beyon memory. in Sna	7 lead cated	https: w.cod ra.org rity-	eauro	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 369	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439 SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279	, bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710, SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2281	https://ww w.qualcom m.com/co mpany/pro duct- security/b	0-QUA-SD_7- 130819/732
NULL Pointer	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip	https://ww w.qualcom	0-QUA-SD_7- 130819/733
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	C ID
Dereference			Snapdr Compu Consur Industr IoT, Sn Snapdr Snapdr MDM9 MDM9 MSM89 QCS400 215, SI SD 425 435, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63 Snapdr	rong blo ragon Au ite, Snap ner IOT, rial IOT, apdrago ragon Vo ragon Vo ragon Vo 5, QCS60 0 210/SI 5, QCS60 0 210/SI 5, QCS60 0 210/SI 5, SD 427 0 439 / S 0 439 / S 0 632, SI 5, SD 712 0 730, SD 712	ito, Snap dragon Snapdra Snapdra in Mobil ice & Mi earables M9206, M9650, SM8996 D5, Qualo D5, Qualo D 212/S 7, SD 430 SD 429, S 5/16/SD D 636, SI C 3D 71 D 820, SI S / SD 71 D 820, SI S / SD 85 DM439, 560, SDX gh_Med	m.cor mpan duct- secur ulletin	y/pro ity/b			
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Ра	tch	NCIIF	PC ID
			SD 632, 675, SD SD 730, 835, SD SD 8CX SDM63 Snapdr SXR113	D 429, S , SD 636) 712 / S , SD 820) 845 / S , SDA66 0, SDA66 agon_Hi 30 : CVE-2	, SD 665 SD 710 / , SD 820 SD 850, S 0, SDM4 560, gh_Med					
Out-of- bounds Write	22-07-2019	7.5	receive lead to issue in Snapdr Compu Consun Industr Mobile, Music, S in MDM MDM96 MDM96 MDM96 MSM89 QCS405 215, SD SD 425, 435, SD SD 425, 665, SD SD 625, 665, SD SD 670, 820A, S 850, SD SDM63 SDX24	d from f an out o video d agon Au te, Snap ner IOT, ial IOT, Snapdra 19150, M 507, MD 550, MSI 96AU, Q 5, QCS60 9210/SI 96AU, Q 5, QCS60 9210/SI 96A27 9439 / S 5D 632 9675, SE 5D 730 5D 835, S	irmwar of bound lriver. ir dragon Snapdra agon Vo gon We (DM920 M9640, M8909V (CA6574 D5, Qualo D 212/S GD 429, S GD 420, S GD	write odragon agon agon ice & arables 06, V, 4AU, comm D 205, 0, SD SD 450, 5, SD SD 710 / 0, SD SD 710 / 0, SD 20, SD SD 710 / 0, SD	w.cod ra.org rity- bullet 19/00	a- ity-	0-QUA- 130819	
Improper Restriction of	22-07-2019	4.6	Out of t due to l	iout	w.cod	://ww leauro g/secu	0-QUA- 130819			
Operations				checking size of input received from WLAN firmware in						,
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 372	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pa	tch	NCIIP	CID
within the Bounds of a Memory Buffer			Consum Industr Mobile, Music in MDM96 QCA657 SD 210, 425, SD SD 450, 665, SD SD 730, 845 / S SDM63 SDX24	/SD 212 427, SD , SD 625 712 / S , SD 820 D 850, S 0, SDM6	Snapdra Snapdra agon Vo 150, M8996A CS405, (/SD 205 0 430, SI , SD 636 D 710 / A, SD 83 D 855, S 60, SDX	agon agon ice & U, QCS605, 5, SD 0 435, 5, SD SD 670, 35, SD SD 670, 35, SD SD 660, 20,	19/0	a- ity-		
Use After Free	25-07-2019	4.6	CVE ID : CVE-2019-2292 Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Integer Overflow or Wraparou nd	25-07-2019	4.6	CVE ID : CVE-2019-2293 An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon				https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code-		0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 373	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
			Mobile, Music, 1 Infrastr in IPQ4 IPQ807 MDM92 MDM92 MDM92 QCA65 QCA93 SD 210 425, SE SD 450 636, SE SD 670 820A, S 850, SE SDX24	:019, IP(74, MDM 206, MD 640, MD 996AU, Q 74AU, Q 77, QCA /SD 212 9 427, SI , SD 600	agon Vo gon Win and Net 28064, 9150, M9607, M9650, QCA6174 CA8081 9379, QU 2/SD 20! 0 430, SI 0 50 625 0 712 / S 0 712 / S 0 820 SD 845 / DM660, S	4A, , CS605, 5, SD 0 435, 5, SD 5D 710 /), SD 2 SD 2 SD 2 SD 2 SD 2 SD 2 SD 2 SD 2	auror secur bullet	ity-		
Out-of- bounds Read	25-07-2019	7.5	reason frame o the fran Snapdr Consum Consum Industr Mobile, Music i MDM92 MSM89 QCA65 QCA93 425, SE SD 450 665, SE SD 670) 427, SI , SD 625	extracte nout val h in tto, Snap tronics napdrag Snapdra Snapdra agon Vo 0150, M9607, M9650, QCA6174 CA9377 405, QCS 0430, SI 5, SD 636 0712 / S	d from idating odragon agon agon bice & 4A, 5605, SD 0 435, 5, SD 5D 710 / 0, SD	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2305		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/740
			CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/741
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptic	on & CVE	ID	Pa	tch	NCIIF	PC ID
			MDM9 QCA61 QCA93 QCS60 205, SI SD 435 625, SI SD 712 730, SI SD 845 SDM63 SDX24		M8996A A6574A 9379, Q 0/SD 21 0 427, SI 0, SD 600 0 665, SI 0 / SD 6 0 820A, 50, SD 85 560, SD 8	AU, U, CS405, 2/SD D 430, 0, SD D 675, 570, SD SD 835, 55, 520,				
N/A	25-07-2019	7.2	CVE ID : CVE-2019-2307 User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Restriction	25-07-2019	4.6	SDM000, SDX20, SDX24CVE ID : CVE-2019-2308When handling the vendor command there exists ahttps://ww w.codeauro0-QUA-SI 130819/*							
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 376	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	july-2019- code- aurora- security- bulletin	
mdm9635n	n_firmware				
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/744
CV Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				377						

Weakness	Publish Date	CVSS	[Descriptio	A30, SDM660, gh_Med_2016, 019-2239 Anination The degraded due oded Snapdragon ton Compute, Insumer IOT, dustrial IOT, G, Snapdragon agon Voice & gon Wearables 1DM9206, M9615, M9635M, M9650, M9650, M8909W, QCS605,		Pat	tch	NCIIP	CID
			QCS404 215, SE SD 410 430, SE SD 450 625, SE 650/52 710 / S SD 820 850, SE SDM43 SDX20, Snapdr SXR113	4, QCS60) 210/SI /12, SD) 435, SE , SD 615) 632, SE 2, SD 675 SD 670, S A, SD 83) 8CX, SI 9, SDM6 , SDX24, agon_Hi 30	95, Quald 9 212/S 425, SD 9 439 / S /16/SD 9 636, SI 5, SD 712 5, SD 712 55, SD 84 9 730, S 5, SD 84 9 730, SD 8 660, 6 30, SD 9 8 Med	comm D 205, 427, SD SD 429, 415, SD D 2 / SD SD 820, 45 / SD 1660, _2016,				
Informatio n Exposure	25-07-2019	7.5	SXR1130 CVE ID : CVE-2019-2239 Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9607, MDM9615, MDM9640, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730,				https: w.qua m.con mpan duct- securi ulletin	n/co y/pro ity/b	0-QUA- MDM9- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publis	h Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
				SDM66	39, SDM 0, igh_Med	·					
				CVE ID	: CVE-2	2019-22	54				
ipq4019_fir	mware	!									
N/A	25-07-	-2019	2.1	surface Error I checke unpred Snapdu Compu Consur Consur Industr IoT, Sn Snapdu Snapdu Infrast in IPQ4 IPQ807 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM	ite, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, apdrago ragon Vo ragon W ructure 1019, IP0 74, MDM 206, MD 640, MD 640, MD 640, MD 640, MD 640, MD 640, MD 640, QCA 74AU, Q 84AU, Q 77, QCA 80, QCA 102, QCS 0/SD 212 0 600, SI 5, SD 712	t to the s is not p s in an behavio ito, Snap dragon napdrag tronics napdrag Snapdra S	screen, roperly ur in odragon gon agon e, usic, working 4A, , , CA9531	w.qua m.con mpan duct- secur ulletin	n/co y/pro ity/b	0-QUA- 130819	-
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

}	3-4
	27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SXR1130		
			CVE ID : CVE-2019-2240		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-IPQ4- 130819/747
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-IPQ4- 130819/748
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			MDM9 MDM9 MSM89 QCA65 QCA93 SD 210 425, SI SD 450 636, SI SD 670 820A, S 850, SI SDX24), SD 730 SD 835, S D 855, SI	M9607, M9650, QCA6174 CA8081 9379, Q 2/SD 20 0 430, SI 0, SD 625 0 712 / S 0, SD 820 SD 845 / DM660, S	4A, , 5, SD D 435, 5, SD SD 710 /), SD / SD SDX20,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	SDX24 CVE ID : CVE-2019-2299 Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	v
ipq8064_fir	mware									
N/A	25-07-2019	2.1	surface Error h checke	sending e content handling d results lictable l	t to the s is not p s in an	screen, roperly	w.qua m.con		0-QUA-IPQ8- 130819/750	
CV Scoring So (CVSS)	cale 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	tch	NCIIP	CID
			Consum Connect Consum Industri IoT, Sna Snapdra Snapdra Infrastri in IPQ40 IPQ807 MDM92 MDM96 MSM89 QCA656 QCA657 QCA658 QCA937	te, Snap tivity, Si her Elec tivity, Si her IOT, ial IOT, apdrago agon Vo agon Wi ucture a 019, IPC 4, MDM 206, MD 96AU, Q 54, QCA 74AU, Q 34AU, Q 34AU, Q 77, QCA 30, QCA 30, QCA 30, QCA 30, QCA 512 50, SD 50, SI 50, SI 50, SI 50, SD 50, SI 50, SD 50, SD	dragon napdrag tronics napdrag Snapdra Snapdra Snapdra Snapdra Snapdra n Mobil nice & M ired and Netv 28064, 9150, M9607, M9607, M9650, QCA6174 6574, CA6584 CA8081 9379, QU 9886, QU 404, QCS 2/SD 20! 2 625, SI 2 / SD 71 D 820, SI 5 / SD 85 DA660, SDX 30	gon agon agon e, usic, working 4A, , , , , , , , , , , , , , , , , , ,	securi			
Use After Free	25-07-2019	4.6	Snapdra Snapdra Snapdra Snapdra	while r ver due ue in Sn agon Co agon Co agon Ind agon Mo agon Wo	eading f e to use a apdrago nnectivi nsumer dustrial obile, earables	rom after on Auto, ity, IOT, IOT,	w.cod ra.org rity-	019- a-	0-QUA- 130819	•
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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 IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263	bulletin	
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-IPQ8- 130819/752
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	escriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			SDX24							
			CVE ID	: CVE-2	019-22	99				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	-
sd_600_firm	iware									
N/A	25-07-2019	2.1	surface Error h checked unpred Snapdr Compu Connec Consum Industr IoT, Sna Snapdr Snapdr Infrast	While sending the renderedsurface content to the screen,Error handling is not properlychecked results in anunpredictable behaviour inSnapdragon Auto, SnapdragonCompute, SnapdragonConnectivity, SnapdragonConsumer ElectronicsConsumer IOT, SnapdragonIndustrial IOT, SnapdragonIoT, Snapdragon Mobile,Snapdragon WiredInfrastructure and Networkingin IPQ4019, IPQ8064,				//ww ilcom n/co y/pro ity/b ns	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
Improper Input Validation	25-07-2019	7.5	SDX24, SXR1130 CVE ID : CVE-2019-2240 Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So	cale 0-1	1-2	2-3	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, SDM660, SDX20		
			CVE ID : CVE-2019-2253		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/756
			CVE ID : CVE-2019-2334 An out-of-bound write can be	https://ww	
Integer Overflow or Wraparou nd	25-07-2019	4.6	triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/757
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/758

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				387						

Weakness	Publish Date	CVSS	De	escriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			SDX24 CVE ID :	CVE-2	019-23	07				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When ha commar potentia to lack o data buf Snapdra Consum Connect Consum Industri Mobile, S Music in MDM96 QCA617 QCA937 QCA617 QCA937 QCS605, 205, SD SD 435, 625, SD SD 712 / 730, SD SD 845 / SDM630 CVE ID :	nd there I buffer I finput fer rece gon Au er Elec ivity, Si er IOT, al IOT, Snapdr 40, MSI 40, MSI 40, MSI 40, MSI 40, MSI 40, MSI 40, MSI 40, SI 50 210 636, SI 636, SI 7 SD 71 820, SI 820, SI 7 SD 85 0, SDM6	e exists a c overflo validati eived in to, Snap tronics napdrag Snapdra Snapdra Snapdra agon Vo 0607, M8996A A6574A 9379, Q0 0/SD 21 0 427, SI 0 427, SI 0 665, SI 0 665, SI 0 / SD 600 0 820A, S 0, SD 85 60, SDX	a ow due on of odragon agon agon ice & U, U, CS405, 2/SD O 430, O, SD O 675, 570, SD SD 835, 55, 24	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
mdm9206_	firmware									
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired				w.qua m.cor	n/co y/pro ity/b	0-QUA- MDM9- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD	
636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2235	
NULL Pointer25-07-20192.1Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Voice & Music, many/prohttps://ww w.qualcom m.com/co O-QU mpany/proNULL Pointer Dereferenc25-07-20192.1Snapdragon Wired Infrastructure and NetworkingMDM	
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	C	escriptio	on & CVE	ID	Pa	tch	NCIIF	PC ID
			Snapdragon_High_Med_2016, SXR1130							
			CVE ID	: CVE-2	2019-22	36				
N/A	25-07-2019	2.1	Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237 Lack of check of data type can				w.qua m.cor	y/pro ity/b	0-QUA- MDM9- 130819	
Out-of- bounds Read	25-07-2019	4.6	Lack of lead to express negativ still eva buffer u Snapdr Compu Consum Consum Industr Mobile MDM90 210/SI 410/12	CVE ID : CVE-2019-2237				://ww alcom n/co ay/pro ity/b ns	0-QUA- MDM9- 130819	9/763
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			710 / SD 670, SD 730, SD 8CX, SXR1130		
			CVE ID : CVE-2019-2238		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MDM9- 130819/764
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an	https://ww w.qualcom m.com/co mpany/pro	O-QUA- MDM9- 130819/765
CV Scoring So (CVSS)	cale 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	Descriptio	n & CVE	ID	Pa	tch	NCIIP	PC ID
			Snapdra Comput Connec Consum Consum Industr IoT, Sna Snapdra Snapdra Snapdra Infrastr in IPQ4 IPQ807 MDM92 MDM92 MDM92 MDM96 QCA652 QCA653 QCA653 QCA653 QCA653 QCA653 QCA653 SD 210, 425, SD SD 675, 670, SD SD 835, 855, SD SDM63 SDX24,	019, IPQ 4, MDM 206, MD 640, MD 96AU, Q 64, QCA 74AU, Q 84AU, Q 77, QCA	ato, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra ired and Netw 28064, 9150, M9607, M9650, 2064, 6574, CA6584 CA6	odragon gon agon agon e, usic, working 4A, 4A, 5, 5, SD 5, S	duct- secur ulleti			
Improper Input Validation	25-07-2019	2.1	backgro check is and also handlin to unin in Snap	renderin ound, Er s not cau o incorre ng is beir tended S odragon A ragon Cor	ror statu 1ght pro ect statu ng done SUI beha Auto, mpute,	us perly is leading aviour	w.qua m.cor	n/co y/pro ity/b	0-QUA- MDM9- 130819	
I I				ugon do		,,				

Weakness	Publish Date	CVSS	0	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			Electro Snapdr Snapdr Snapdr Infrastr in MDM MDM90 QCS404 212/SI 636, SI SD 670 820A, S 850, SI	, SD 730 SD 835, S O 855, SD O, SDM6	nectivit nsumer dustrial obile, red and Netv 1DM920 M9650, M8996A 05, SD 22 0 410/1 0 712 / S , SD 820 5D 845 / 0 8CX, SI	y, IOT, IOT, Working 06, U, 10/SD 2, SD 5D 710 / 0, SD 7 SD DA660,				
			Possibl		overflo	w at the				
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835,				w.qua m.con	n/co y/pro ity/b	0-QUA- MDM9- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 393	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			SDA660, SDM439, SDM630, SDM660			
Improper Input Validation	25-07-2019	7.5	CVE ID : CVE-2019-2243 Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/768	
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MDM9- 130819/769	
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	Description & CVE ID		Patch		NCIIP	CID		
			MDM9 MDM9 Qualco 212/SI SD 430 429, SI 415, SI SD 650 712 / S SD 820 845 / S SDA66 SDA66 Snapdr SXR113	5D 710 / 5D 820 5D 850, S 0, SDM4 50, SDX2 50, SDX2 50, SDX2 50, SDX2 50	M9650, M8909V (CS605, , SD 210 0 425, SI , SD 439 0 615/10 0 632, SI 665, SD SD 670, A, SD 83 39, SDM 0, gh_Med	V,)/SD) 427,) / SD 6/SD) 636, 675, SD SD 730, 35, SD SD 8CX, 630, _2016,				
Use After Free	22-07-2019	6.9	SXR1130 CVE ID : CVE-2019-2254 A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24,			w.cod	5/03/ 2019- a- ity-	0-QUA- MDM9- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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			
			CVE ID : CVE-2019-2260			
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MDM9- 130819/771	
			CVE ID : CVE-2019-2261			
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code-	O-QUA- MDM9- 130819/772	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263	aurora- security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA- MDM9- 130819/773
NULL Pointer Dereferenc	25-07-2019	7.8	Null pointer dereferencing canhttps://wwhappen when playing the clipw.qualcomwith wrong block group id inm.com/co		O-QUA- MDM9- 130819/774
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
e			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334 Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon					y/pro ity/b ns		
Out-of- bounds Write	22-07-2019	7.5	received from firmware can lead to an out of bound write issue in video driver. in				w.cod ra.org rity- bullet	a- ity-	0-QUA- MDM9- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Use After Free25-07-20194.6MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD A30, SD 435, SD 450, SD 625, SD 712 / SD 636, SD 650/52, SD 712 / SD 636, SD 650/52, SD 712 / BUIletincode- aurora- security- bulletinUse After Free25-07-20194.6Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon Mobile,https://ww w.qualcom m.com/coUse After Free25-07-20194.6Snapdragon Consumer IOT, Snapdragon Mobile,0-QUA- mpany/pro MDM9- 130819/777	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free25-07-20194.6Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables in MDM9640, MDM9607, MDM9640, MDM9650, MDM9640, MDM9650, MDM9640, MDM9650, SD 636, SD 650/52, SD 712 / SD 710 / SD 710 / S				665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,		
Use After Free25-07-20194.6multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables in MDM9640, MDM9650, WDM9640, MDM9650, WDM9640, MDM9650, WDM9640, Sp 430, SD 425, SD 427, SD 				CVE ID : CVE-2019-2287		
Use After Free25-07-20194.6accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute,https://ww w.qualcom m.com/co0-QUA- MDM9- 130819/777 Snapdragon Mobile,		25-07-2019	4.6	multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	č
Snapdragon Voice & Music,ulletinsSnapdragon Wearables inMDM9150, MDM9206,		25-07-2019	4.6	accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	w.qualcom m.com/co mpany/pro duct- security/b	e
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		cale 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	on & CVE	ID	Pa	tch	NCIIP	C ID	
			MDM9 QCS40 212/SI SD 430 625, SI SD 670 845 / S SDM66	607, MD 650, MS 5, QCS6(D 205, SI 0, SD 435 D 636, SI 0, SD 820 SD 850, S 50, SDX2 0 : CVE-2	M8909V 05, SD 22 5, SD 425, SD 5, SD 450 0 712 / S 0, SD 820 SD 855, 0, SDX24	10/SD D 427,), SD SD 710 /)A, SD 4					
Integer Overflow or Wraparou nd	25-07-2019	4.6	trigger comma usersp Snapdn Consur Consur Indust Mobile Music, Infrast in IPQ4 IPQ807 MDM9 MDM9 MDM9 MDM9 MSM89 QCA65 QCA93 SD 210 425, SI SD 450 636, SI SD 670 820A, SI SDX24	and supp ace appl ragon Au mer Elec ctivity, S mer IOT, rial IOT, , Snapdr Snapdra ructure 4019, IP0 74, MDM 206, MD 640, MD 640, MD 996AU, Q 77, QCA 0, SD 600 0, SD 600 0, SD 730 SD 835, SI 0, S5, SI	specially lied by a ication. ito, Snap tronics napdrag Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra (Snapdra Snapdra Snapdra (Snapdra Snapd	r-crafted a in odragon agon agon ice & red working 4A, , CS605, 5, SD 0 435, 5, SD 50 710 / 0, SD 5D 710 / 0, SD 5DX20,	w.cod ra.org rity- bullet 19/02	a- ity-	0-QUA- MDM9- 130819	/778	
Out-of- bounds	25-07-2019	7.5	CVE ID : CVE-2019-2299 Out of bound access when reason code is extracted from				-	//ww leauro	-		
CV Scoring S (CVSS)	cale 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	Pa	tch	NCIIP	CID
Read			the fran Snapdr Consur Consur Industr Mobile Music i MDM92 MDM92 QCA65 QCA93 425, SE SD 450 665, SE SD 670 820A, S 850, SE SDM66	data with me lengt ragon Au ner Elect ctivity, Sn ner IOT, rial IOT, 3 , Snapdra 640, MD 206, SD 206, SD 206, SD 20675, SD 20675, SD 20675, SD 20855, SD 20855, SD 200, SDX20 200, SDX20 200, SDX20 200, SDX20 200, SDX20 200, SDX20 200, SDX20 200, SDX20	h in ito, Snap tronics napdrag Snapdra agon Vo 9150, M9607, M9650, QCA6174 CA9377 405, QCS 0 430, SI 5, SD 636 0 712 / S 0, SD 820 SD 845 / DA660, S 0, SDX24	odragon gon agon agon oice & 4A, 5605, SD 0 435, 5, SD 5D 710 / 0, SD 5D 710 / 0, SD 5DM630, 4	rity-	2019- a- ity-	130819	/779
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675,				w.cod ra.org rity- bullet	a- ity-	0-QUA- MDM9- 130819	/780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/781
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code-	O-QUA- MDM9- 130819/782
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 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 Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20	aurora- security- bulletin	
mdm9607_1		CVE ID : CVE-2019-2309			
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/783
CV Scoring So					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				403						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2235		
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MDM9- 130819/784
			CVE ID : CVE-2019-2236		
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/785
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 404	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237		
Out-of- bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2238	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/786
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/787
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 405	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descriptio	on & CVE I	D	Pa	tch	NCIIP	CID
			Connectivity, S Consumer IOT Industrial IOT, Mobile, Snapdra Music, Snapdra Infrastructure in MDM9150, I MDM9607, ME MDM9640, ME MDM9655, MS QCS404, QCS60 215, SD 210/S SD 410/12, SD 430, SD 435, SI SD 450, SD 615 625, SD 632, SI 650/52, SD 632, SI 650/52, SD 677 710 / SD 670, SI SD 820A, SD 83 850, SD 8CX, SI SDM439, SDM6 SDX20, SDX24, Snapdragon_H SXR1130 CVE ID : CVE-2	C, Snapdra ragon Vo agon Wir and Netv MDM920 DM9635M DM9650, SM8996A 05, Qualc 5D 212/SI D 439 / S 5/16/SD D 636, SE 5, SD 712 SD 730, S 35, SD 84 DA660, 630, SDM c, ligh_Med_	agon Igon ice & red working IG, 4, U, comm D 205, 427, SD SD 429, 415, SD D 2 / SD SD 820, ISD 820,				
N/A	25-07-2019	2.1	While sending surface conten Error handling checked result unpredictable Snapdragon Au Compute, Snap Connectivity, S Consumer Elec Consumer IOT Industrial IOT, IoT, Snapdragon Vo	w.qua m.con	n/co y/pro ity/b	0-QUA- MDM9- 130819			
			Snapdragon W Infrastructure		vorking				

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
			IPQ807 MDM99 MDM99 QCA65 QCA65 QCA65 QCA65 QCA93 QCA98 QCN55 SD 210 425, SI SD 675 670, SI SD 835 855, SI SDM63 SDX24,	80, QCA 02, QCS 0/SD 212 0 600, SI 5, SD 712 0 730, SI 5, SD 845 0 8CX, SI 80, SDM6 , SXR113	19150, 19950, 199607, 199650, 2006174, 2006584 2006584 2006584 20079, Q 9886, Q 404, QC 20071 20820, S1 20820, S1 20820, S1 50860, 560, SDX 30	4A, , , CA9531, CA9980, S605, 5, SD D 636, L0 / SD D 820A, 50, SD				
Improper Input Validation	25-07-2019	2.1	CVE ID : CVE-2019-2240While rendering the layoutbackground, Error statuscheck is not caught properlyand also incorrect statushandling is being done leadingto unintended SUI behaviourin Snapdragon Auto,Snapdragon Compute,Snapdragon Connectivity,Snapdragon ConsumerElectronics Connectivity,Snapdragon Industrial IOT,Snapdragon Mobile,Snapdragon WiredInfrastructure and Networkingin MDM9150, MDM9206,MDM9655, MSM8996AU,QCS404, QCS605, SD 210/SD212/SD 205, SD 410/12, SD				w.qua m.cor	n/co y/pro ity/b	0-QUA- MDM9- 130819	/789
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130		
			CVE ID : CVE-2019-2241		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/790
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/791
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 408	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MDM9- 130819/792
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/793
			CVE ID : CVE-2019-2260 Unauthorized access from GPU		
N/A	22-07-2019	4.9	subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/794
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 410	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	PC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261 Access to freed memory can							
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD		w.cod ra.org rity- bullet	a- ity-	0-QUA- MDM9- 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	CID
			SD 845 SDX20 Snapdr	0 820, SI 6 / SD 85 , ragon_Hi 0 : CVE-2	0, SDM	560, _2016				
NULL Pointer Dereferenc e	22-07-2019	4.6	occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264				w.cod ra.org rity- bullet	a- ity-	0-QUA- MDM9- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845				w.cod ra.org rity- bullet	a- ity-	0-QUA- MDM9- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/ SD 850, SDM660, SDX20		
			CVE ID : CVE-2019-2272		
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/798
Improper Authentica tion	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 CVE ID : CVE-2019-2278	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/799
Improper Restriction of Operations within the	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity,	https://ww w.codeauro ra.org/secu rity- bulletin/20	O-QUA- MDM9- 130819/800

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				/112						

Γ

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
Bounds of a Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279					a- ity-		
NULL Pointer Dereferenc e	25-07-2019	7.8	happer with w Snapdr Compu Consur Industr IoT, Sn Snapdr MDM9 MSM89 QCS409 215, SI SD 425 435, SI SD 600 625, SI	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD		w.qua m.cor	n/co y/pro ity/b	0-QUA- MDM9- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016		
			CVE ID : CVE-2019-2334		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/802
				https://www	
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-	O-QUA- MDM9- 130819/803
CV Scoring So (CVSS)	cale 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	I	Description & CVE ID				tch	NCIIP	CID
				MDM9 MDM9 MSM89 QCS60 430, SI SD 636 SD 710 820A, SI 850, SI Snapdi	ragon W 206, MD 640, MD 909W, M 5, SD 42 0 435, SI 6, SD 650 0 / SD 67 SD 835, S 0 8	M9607, M9650, SM8996 5, SD 42 O 450, SI 0/52, SD 70, SD 82 SD 845 SD 845 SDX20, S	6AU, 7, SD D 625, 712 / 20, SD / SD SDX24, _2016	secur bullet			
Use After Free	25-0	7-2019	4.6	accessi macro after-fi Snapdi Snapdi Snapdi Snapdi Snapdi MDM9 MDM9 QCS40 212/SI SD 430 625, SI SD 670 845 / S	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24		w.qua m.cor mpan duct- secur ulletin	y/pro ity/b	0-QUA- MDM9- 130819		
Integer Overflow or Wraparou nd	25-0	7-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon				w.cod ra.org rity- bullet 19/02	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019-		/805
CV Scoring So (CVSS)	cale	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	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299 Out of bound access when reason code is extracted from				code- auror secur bullet	ity-		
Out-of- bounds Read	25-07-2019	7.5	reason frame of the fran Snapdr Consum Connect Consum Industr Mobile, Music i MDM92 MSM89 QCA65 QCA93 425, SD SD 450	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 /		w.cod ra.org rity- bullet	a- ity-	0-QUA- MDM9- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	<mark>3-4</mark> 417	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA- MDM9- 130819/807
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA- MDM9- 130819/808
CV Scoring So	cale 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	Pa	tch	NCIIF	PC ID
			MDM9 MDM9 QCA61 QCA93 QCS60 205, SI SD 435 625, SI SD 712 730, SI SD 845 SDM63 SDX24	150, MD 607, MD 650, MS 74A, QC 77, QCA 5, SD 21 0 425, SI 0 425, SI 5, SD 450 0 636, SI 2 / SD 71 0 820, SI 3 820, SD 8 0, SDM6	M9640, M8996A A6574A 9379, Q 0/SD 21 0 427, SI 0, SD 600 0 665, SI 0 / SD 6 0 820A, 3 50, SD 85 560, SDX	U, U, CS405, 2/SD D 430, 0, SD D 675, 570, SD SD 835, 55, 520,				
N/A	25-07-2019	7.2	User ap potenti the fast driver to go th subsys Auto, S IOT, Sn IOT, Sn IOT, Sn Snapdr MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM	oplicatio ially mal trpc driv will allo nrough t tem in S napdrago apdrago ragon Vo 5, Qualco 5, Qualco 5, Qualco 0, SD 42 0, SD 42 0, SD 712 0, SD 72 0,	on could ke RPC of ver and t w the m o the rep napdrag gon Cons on Indus on Mobil oice & M earables M9607, M8909V QCS405, Omm 21 O 430, SI 29, SD 45 O 636, SI 29, SD 45 O 636, SI 20, SD 71 O 820A, 3 50, SD 85 39, SDM 0, SDX2	all to the essage mote gon sumer trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, usic, trial e, tria e, trial e, trial e, trial e, trial e, trial e, tria e tria e t tria e tria e t tria e tria e t tria e tria e t tria e tria e t tria e tria e t tria e t tria e t tria e t tria e tria e to tria e t tria tria tria tria e to tria tria tria tria tria tria tria tria	w.cod ra.org rity- bullet	a- ity-	0-QUA- MDM9- 130819	
Out-of-	25-07-2019	7.5	While storing calibrated data			https:	//ww	0-QUA-		
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4 /19	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Ра	tch	NCIIP	CID
bounds Read			integer since d exceed Snapdr Consur Consur Industr Mobile Music i MDM9 MSM89 QCA65 QCA93 205, SI SD 712 820A, S SDM66	rmware overflow ata lengt real data ragon Au ner Elect ctivity, Sr ner IOT, rial IOT, snapdra (Snapdra 206, MD 206, MD	w may c th receiv a length to, Snap tronics napdrag Snapdra Snapdra agon Vo 0150, M9607, M9650, 02A6174 CA9377 10/SD 2 0 625, SI 0 / SD 6 SD 850 0	AA, 4A, 212/SD 0 636, 70, SD ,	ra.org rity- bullet	a- ity-	MDM9- 130819	/810
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When I comma potenti to lack data bu Snapdr Consur Consur Industr Mobile Music i MDM9 QCA61 QCA93 QCS60 205, SI SD 435 625, SI	e: CVE-2 nandling and there ial buffer of input affer rece ragon Au ner Elect ctivity, Su ner IOT, rial IOT, rial IOT, frial IOT, fr	the ven e exists a validati eived in to, Snap tronics napdrag Snapdra Snapdra Snapdra Snapdra 2007, W8996A A6574A 9379, Q 0/SD 21 0 427, SI , SD 600 0 665, SI	dor a ow due on of odragon agon agon ice & U, U, CS405, 2/SD D 430, D 675,	w.cod ra.org rity- bullet	a- ity-	0-QUA- MDM9- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 420	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			SD 845 SDM63	0 820A, 3 0, SD 85 660, SDX	5, 24					
			CVE ID	: CVE-2	019-23	12				
mdm9650_f	firmware									
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	emulat sector s TA roll Snapdr Compu Consur Consur Consur Industr Mobile Music, Infrastr in MDM MSM89 QCS609 410/12 430, SE SD 450 636, SE SD 820 845 / S SDM43 Snapdr SXR113 CVE ID), SD 820 SD 850, S 39, SDM6 ragon_Hi 30 • : CVE-2	B is used imption otection ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra agon Vo gon Win and Net 1DM960 M9655, QCS404, 0M9655, QCS404, 5, SD 42 0 439 / S 5, SD 42 0 439 / S 5, SD 42 0 710 / A, SD 83 50 8CX, S 50 8CX, S	l due to s in the logic. in odragon gon agon ice & red working 07, 5, SD 7, SD 5, SD 7, SD 5D 429, 2, SD SD 670, 35, SD SD 670, 35, SD SD 670, 35, SD SD 670, 35, SD	w.qua m.con	n/co y/pro ity/b	0-QUA- MDM9- 130819	
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer				w.qua m.con	n/co y/pro	0-QUA- MDM9- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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 IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236	ulletins	
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/814

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				422						

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	Pa	tch	NCIIP	C ID	
			SXR11	30						
			CVE ID) : CVE-2	2019-22	37				
Out-of- bounds Read	25-07-2019	4.6	lead to expres negative still events buffer Snapdir Comput Consum Consum Industr Mobile MDM9 210/SI 410/12 710 / S SXR11	aluate to underflo ragon Au ite, Snap ner Elec ctivity, S ner IOT, rial IOT, in MDM 607, MD 655, QC 0 212/S 2, SD 67, S	aent loo entially ne condi o true lea ow. in ato, Snap dragon tronics napdrag Snapdra Snapdra 19206, M9650, S605, SE D 205, S 5, SD 71 SD 730, S	p- go tion will ading to odragon gon agon agon D 2 / SD SD 8CX,	w.qua m.cor	n/co y/pro ity/b	0-QUA- MDM9- 130819	/815
Improper Input Validation	25-07-2019	2.1	layout Corrup Denial Snapdu Compu Connee Consur Indust Mobile Music, Infrast in MDM MDM9	ite, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, , Snapdr Snapdra	an lead t can lead tc in ito, Snap dragon napdrag tronics napdrag Snapdr Snapdr Snapdra agon Vc agon Win and Net MDM920 M96350,	to SUI to odragon gon agon agon oice & red working 06, M,	w.qua m.cor	n/co y/pro ity/b	O-QUA- MDM9- 130819	/816
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Vired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA9886, QCA9980,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/817
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9206, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2241	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MDM9- 130819/818
Improper Restriction	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while	https://ww w.qualcom	O-QUA- MDM9-
CV Scoring So (CVSS)	cale 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	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
of Operations within the Bounds of a Memory Buffer			lead to in Snap Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Music, S in MDM MDM96 MSM89 210/SD SD 427, 439 / S 615/16 632, SD SD 712 730, SD SD 845 SDA660 SDM66	the vers information agon Contagon Lond agon Contagon Ind agon Ind agon Ind agon Ind agon Ion Snapdra (19206, M (50, MSN (96AU, Q (96AU, S (96AU, S) (96AU, S (96AU, S) (96AU, S (96AU, S) (96AU, S) (9	tion dise Auto, mpute, nsumer lustrial C, Snapd agon Vo gon Wea IDM960 M8909W (CS605, 0 205, SI 0 450, SI 0 450, SI 0 450, SI 0 450, SI 0 665, SI 0 665, SI 0 820A, S 0 820A, S 0, SD 85 39, SDM	closure. IOT, IOT, ragon ice & arables 7, V, SD 0 425, 5, SD 0 425, 5, SD 5, SD 5, SD 0 675, 70, SD 50 835, 5, 630,	m.con mpan duct- secur ulletin	y/pro ity/b	130819	/819
Improper Input Validation	25-07-2019	7.5	while p corrupt Snapdry Connec Consum Industry IoT, Sna Snapdry Snapdry MDM94 MDM94 MSM89 QCS405 215, SD SD 425, 435, SD	over-rea barsing a ted comm agon Au tivity, Sr ner IOT, tial IOT, S apdragon agon Vo agon Vo agon We 5, QCS60 0 210/SE , SD 427 0 439 / S , SD 615	n ogg fil nent blo to, Snap napdrag Snapdra Snapdra n Mobilo ice & Mu earables M9206, M9650, SM8996 5, Qualo 212/SI , SD 430 D 429, S	e with a ock. in odragon agon agon e, usic, in 5AU, comm D 205, 0, SD 5D 450,	https: w.qua m.con duct- secur ulletin	n/co y/pro ity/b	O-QUA- MDM9- 130819	/820
CV Scoring Sc	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Inf, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDX20, SDA660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MDM9- 130819/821
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free	https://ww w.codeauro ra.org/secu	O-QUA- MDM9- 130819/822
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 427	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra MDM96 MDM96 QCS405 215, SD SD 425, 435, SD SD 425, 435, SD SD 625, 665, SD SD 730, 845 / S SDM43 ^a SDX20, Snapdra SXR113	, SD 820 D 850, S 9, SDM6 SDX24, agon_Hij	ompute, onsumer dustrial obile, oice & Mu earables M9206, M9640, M8909V 05, Qualo D 212/SI 7, SD 430 SD 429, S 2, SD 636 SD 710 / 0A, SD 83 SD 855, S30, SDM	IOT, IOT, usic, in V, comm D 205, 0, SD SD 450, 5, SD SD 670, 35, SD 1660, _2016,		a- ity-		
N/A	22-07-2019	4.9	subsyst non sec can lead disclosu Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra MDM92 MDM96 QCA808	d to info ure in Sr agon Co agon Co agon Co agon Mo agon Mo agon Wi	ILOS or o system i ormation napdrag ompute, onnectivi onsumer dustrial obile, oice & Mi ired and Netw DM9150 M9607, M8996A 605, Qua	other memory on Auto, ty, IOT, IOT, usic, working , .U, .U,	w.qua m.con	n/co y/pro ity/b	O-QUA- MDM9- 130819	
CV Scoring Sc										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA- MDM9- 130819/824
Improper Restriction of Operations	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length	https://ww w.codeauro ra.org/secu rity-	0-QUA- MDM9- 130819/825
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 429	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	Description & CVE ID		Pat	tch	NCIIPC ID		
within the Bounds of a Memory Buffer			Snapdra Snapdra Snapdra Snapdra MDM91 MSM899 QCS605 665, SD SD 730, 835, SD SDA660 SDX20,	agon Coi agon Coi agon Ind agon Mo agon Voi 50, MDI 96AU, Q 5, SD 625 712 / S SD 820, 845 / S 0, SDM63 SDX24, S	mpute, nsumer lustrial bile, ice & Mu M9650, CS405, 5, SD 63 D 710 / SD 820 D 710 / SD 820 D 850, SD 30, SDM SXR113	IOT, usic in 6, SD SD 670, 0A, SD SD 855, 6660, 0	bullet 19/06 june-2 code- auror securi bullet	5/03/ 2019- a- ity-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2269 Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 8455 / SD 850, SDM660, SDX20			w.cod ra.org rity- bullet	in/20 7/01/ 019- a- ity-	0-QUA- MDM9- 130819	/826	
Improper Restriction of Operations within the	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity,			https://ww w.codeauro ra.org/secu rity- bulletin/20		O-QUA- MDM9- 130819/827		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIP	CID	
Bounds of a Memory Buffer			Snapdragon Consumer IOT Snapdragon Industrial IOT Snapdragon Mobile, Snapdragon Voice & Music Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU QCS405, QCS605, Qualcom 215, SD 210/SD 212/SD 20 SD 425, SD 439 / SD 429, S 450, SD 625, SD 632, SD 63 SD 665, SD 675, SD 712 / S 710 / SD 670, SD 730, SD 8 SD 820A, SD 835, SD 845 / 850, SD 855, SDA660, SDM SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_20 CVE ID : CVE-2019-2279	C, june-2019- code- aurora- security- bulletin J, J, MM 05, SD 36, SD 320, Y SD [439,			
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing happen when playing the o with wrong block group id Snapdragon Auto, Snapdra Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU QCS405, QCS605, Qualcom 215, SD 210/SD 212/SD 20 SD 425, SD 427, SD 430, SI 435, SD 439 / SD 429, SD 4 SD 600, SD 615/16/SD 413 625, SD 632, SD 636, SD 66 SD 675, SD 712 / SD 710 / 670, SD 730, SD 820, SD 820	clip in agon n n h ttps://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins 05, 0 5, SD 55, SD	O-QUA- MDM9-	•	
CV Scoring So (CVSS)	cale 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 & CVE ID	Patch	NCIIPC ID	
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016			
			CVE ID : CVE-2019-2334			
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA- MDM9- 130819/829	
				https://www		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-	O-QUA- MDM9- 130819/830	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290	security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/831
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/832
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 433	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24		
Integer Overflow or Wraparou nd	25-07-2019	4.6	CVE ID : CVE-2019-2298 An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA- MDM9- 130819/833

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				434						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2299		
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/834
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/835
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA- MDM9- 130819/836
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message	https://ww w.codeauro ra.org/secu rity-	O-QUA- MDM9- 130819/837
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 436	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308	bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	
Out-of- bounds Read	25-07-2019	7.5	CVE ID : CVE-2019-2308While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/838

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				437						

Weakness	Publish Date	CVSS	Description & CVE	D Patch	NCIIPC ID)
			SDM660, SDX20			
			CVE ID : CVE-2019-23	09		
mdm9655_1	firmware				· · · · · · · · · · · · · · · · · · ·	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs emulated RPMB is used sector size assumptions TA rollback protection Snapdragon Auto, Snap Compute, Snapdragon Connectivity, Snapdrag Consumer Electronics Connectivity, Snapdrag Consumer IOT, Snapdra Industrial IOT, Snapdra Mobile, Snapdragon Vo Music, Snapdragon Wir Infrastructure and Netv in MDM9206, MDM9600 MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 213 410/12, SD 425, SD 427 430, SD 435, SD 439 / S SD 450, SD 625, SD 632 636, SD 712 / SD 710 / SD 820, SD 820A, SD 83 845 / SD 850, SD 8CX, S SDM439, SDM630, SDM Snapdragon_High_Med_ SXR1130 CVE ID : CVE-2019-22	due to s in the logic. in dragon on on gon ice & vorking 7, 5, SD 5, SD	om co O-QUA- pro MDM9- 130819/83	19
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using spect application ids. in Snap Auto, Snapdragon Comp Snapdragon Connectivit Snapdragon Consumer Electronics Connectivit Snapdragon Consumer	on https:// ific w.qualco dragon m.com/o pute, mpany/ ty, duct- security y, ulletins	om co 0-QUA- pro MDM9- 130819/84	0
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8 8-9 9-	-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2236		
N/A	25-07-2019	2.1	Failure in taking appropriateaction to handle the error caseIf keypad gpio deactivationfails leads to silent failurescenario and subsequent logicgets executed everytime inSnapdragon Auto, SnapdragonCompute, SnapdragonConsumer ElectronicsConnectivity, SnapdragonIndustrial IOT, SnapdragonMobile in MDM9206,MDM9607, MDM9650, SD210/SD 212/SD 205, SD210/SD 212/SD 205, SD710 / SD 670, SD 730, SD 8CX,SXR1130CVE ID : CVE-2019-2237	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/841
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
Out-of- bounds Read	25-07-2019	4.6	lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2238					//ww ilcom n/co y/pro ity/b ns	0-QUA- MDM9- 130819	
Improper Input Validation	25-07-2019	2.1	layout Corrup Denial Snapdr Compu Connec Consur Consur Industr Mobile Music, Infrastr in MDM MDM90 MDM90 QCS404	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,				//ww ilcom n/co y/pro ity/b ns	0-QUA- MDM9- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	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
			430, SD 435, SD 439 / S SD 450, SD 615/16/SD 625, SD 632, SD 636, SI 650/52, SD 675, SD 712 710 / SD 670, SD 730, S SD 820A, SD 835, SD 84 850, SD 8CX, SDA660, SDM439, SDM630, SDM SDX20, SDX24, Snapdragon_High_Med SXR1130 CVE ID : CVE-2019-22	415, SD 2 / SD 5D 820, 5 / SD 1660, _2016,			
Improper Input Validation	25-07-2019	2.1	While rendering the lay background, Error statt check is not caught pro and also incorrect statu handling is being done to unintended SUI beha in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivit Snapdragon Consumer Electronics Connectivit Snapdragon Consumer Snapdragon Industrial Snapdragon Industrial Snapdragon Mobile, Snapdragon Wired Infrastructure and Netv in MDM9150, MDM9200 MDM9607, MDM9650, MDM9655, MSM8996A QCS404, QCS605, SD 212 212/SD 205, SD 410/112 636, SD 675, SD 712 / S SD 670, SD 730, SD 8200 820A, SD 835, SD 845 / 850, SD 855, SD 8CX, SI SDM630, SDM660, SDX SXR1130 CVE ID : CVE-2019-222	us perly is leading wiour ty, 10T, 10T, 10T, 10T, 10T, 10T, 10T, 10T	lcom n/co y/pro ity/b	0-QUA- MDM9- 130819	/844
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descrip	otion & CVE	ID	Pa	tch	NCIIP	CID
Informatio n Exposure	25-07-2019	7.5	to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254		w.qua m.con	n/co y/pro ity/b	0-QUA- MDM9- 130819		
msm8996a	u_firmware								
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon			w.qua m.con	n/co y/pro ity/b	0-QUA- MSM8- 130819	
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130							
NULL Pointer Dereferenc e	25-07-2019	2.1	Null po during termin applica Auto, S Snapdr	e: CVE-2 inter des secure a ation usi ition ids. napdrag ragon Co ragon Co ragon Co ragon Co ragon Co ragon Mo ragon Mo ragon Wi ragon Wi ragon Wi ragon Wi ragon Wi ragon Wi ragon Wi ragon SC ragon SC rag	reference application ing spection in Snap on Com nnectivit nsumer inectivit nsumer dustrial obile, ice & Mu ice & Mu ic	ce on ific dragon pute, ity, ity, IOT, IOT, IOT, usic, usic, working , U, ilcomm 5, SD 0 439 / 5, SD 2, SD 2, SD	w.qua m.con mpan duct- secur ulletin	n/co y/pro ity/b ns	0-QUA- MSM8- 130819	/847
CV Scoring Sc (CVSS)	cale 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	ſ	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
				SD 730 835, SI SDM43	5D 710 /), SD 82(DA660, 530, SDN igh_Med	1660,					
				CVE ID	: CVE-2	2019-22	36				
Improper Input Validation	25-07	-2019	2.1	layout Corrup Denial Snapdn Compu Connec Consur Industr Mobile Music, Infrast in MDM MDM9 MDM9 MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52 710 / S SD 820 850, SI SDM43 SDX20 Snapdn SXR112	which c of Servi agon Au agon Au te, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, snapdra ructure /9150, I 607, MD 640, MD 655, MS 4, QCS60 0 210/S 0 210/S	ato, Snap odragon napdrag ctronics napdrag Snapdra Snapdra agon Vin and Net MDM920 M96351 M9650, M9650, M8996A D5, Qual D 212/S 425, SD 0 439 / S 5, SD 71 SD 730, S 35, SD 84 DA660, 630, SDN	ao SUI to odragon gon agon agon agon agon agon agon a	w.qua m.con	n/co y/pro ity/b	0-QUA- MSM8- 130819	/848
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	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	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6584AU, QCA6174A, QCA6584AU, QCA6384, QCA6584AU, QCA6574, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9880, QCA95502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, <t< td=""><td>https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins</td><td>0-QUA- MSM8- 130819/849</td></t<>	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MSM8- 130819/849
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading	https://ww w.qualcom m.com/co mpany/pro duct-	O-QUA- MSM8- 130819/850
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 445	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptic	on & CVE	ID	Pa	tch	NCIIP	CID
			in Snap Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Infrast in MDM MDM9 QCS40 212/SI 636, SI SD 670 820A, S 850, SI SDM63 SXR113	49150, N 607, MD 655, MS 4, QCS6(0 205, SI 0 675, SI 0 675, SI 50 835, S 80, SDM6	Auto, ompute, onnectivionsumer onsumer dustrial obile, ired and Net MDM920 M9650, M8996A D5, SD 22 D 410/1 D 712 / S D 820 SD 845 / D 8CX, S 560, SDX	ity, y, IOT, IOT, IOT, Working 06, U, 2, SD 2, SD 5D 710 / 0, SD 2 SD 2 A660, 24,	secur	• •		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	end of getting lead to in Snap Snapdr Snapdr Snapdr Mobile Music, in MDM MDM9 MSM89 210/SI SD 427 439 / S	le buffer iterating informa odragon ragon Co ragon Co ragon Io ragon Io , Snapdra A9206, M 650, MS 996AU, C 0 212/SI 7, SD 430 50 429, S 6/SD 41	g loop w sion info ation dis Auto, ompute, onsumer dustrial T, Snapo agon Vo agon We MDM960 M8909V QCS605, D 205, S D 205, S SD 450, S	hile and closure. IOT, IOT, Iragon ice & arables 07, V, SD D 425, 5, SD SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- MSM8- 130819	
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660		
			CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MSM8- 130819/852
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MSM8- 130819/853
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 447	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD	https://w w.qualcom m.com/co mpany/pr duct- security/h	m 0-QUA- ro MSM8- 130819/854
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MSM8- 130819/855
Improper Restriction of Operations	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length	https://ww w.codeauro ra.org/secu rity-	O-QUA- MSM8- 130819/856
within the CV Scoring Sc	cale 0-1	1-2	validation in Snapdragon Auto,2-33-44-55-6	6-7 7-8	8-9 9-10
(CVSS)	0-1	1-2	449	0, 70	0.5 25-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269	19/06/03/ june-2019- code- aurora- security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MSM8- 130819/857
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/	O-QUA- MSM8- 130819/858
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIP	CID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276 Out of bound read can happen				july-2 code- auror secur bullet	a- ity-		
Out-of- bounds Read	22-07-2019	4.6	CVE ID : CVE-2019-2276 Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277		w.cod ra.org rity- bullet	a- ity-	0-QUA- MSM8- 130819			
Improper Restriction of Operations within the Bounds of a Memory	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,				w.cod ra.org rity- bullet	//ww leauro g/secu cin/20 6/03/ 2019-	O-QUA- MSM8- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279	code- aurora- security- bulletin	
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id inSnapdragon Auto, SnapdragonCompute, SnapdragonConsumer IOT, SnapdragonIndustrial IOT, SnapdragonIoT, Snapdragon Mobile,Snapdragon Voice & Music,Snapdragon Wearables in MDM9150, MDM9206,MDM9607, MDM9650,MSM8909W, MSM8996AU,QCS405, QCS605, Qualcomm215, SD 210/SD 212/SD 205,SD 425, SD 427, SD 430, SD435, SD 439 / SD 429, SD 450,SD 600, SD 615/16/SD 415, SD625, SD 632, SD 636, SD 665,SD 675, SD 712 / SD 710 / SD670, SD 730, SD 820, SD 820A,SD 835, SD 845 / SD 850, SD855, SDA660, SDM439,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MSM8- 130819/861
CV Scoring So	cale 0-1	1-2	2-3 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, SDM660, SDX20, Snapdragon_High_Med_2016		
			CVE ID : CVE-2019-2334		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, Snapdragon_High_Med_2016, SXR1130	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MSM8- 130819/862
Congregation			CVE ID : CVE-2019-2343	https://	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	O-QUA- MSM8- 130819/863
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24	bulletin	
			CVE ID : CVE-2019-2345		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA- MSM8- 130819/864
			Multiple open and close from	https://ww	
Use After Free	25-07-2019	4.6	multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	nttps://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-	O-QUA- MSM8- 130819/865
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290	security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA- MSM8- 130819/866
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code-	O-QUA- MSM8- 130819/867
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			Mobile Music, Infrast in IPQ4 IPQ807 MDM9 MDM9 MSM89 QCA65 QCA93 SD 2100 425, SI SD 2100 425, SI SD 4500 636, SI SD 6700 820A, SI SDX24	rial IOT, , Snapdr Snapdra ructure a 4019, IP(74, MDM 206, MD 206, MD 206, MD 206, MD 206, MD 206, MD 206, MD 206, MD 206, SI 207, QCA 77, QCA 77, QCA 77, QCA 77, QCA 77, QCA 75, SI 0, SD 730 50 835, SI 0 855, SI	ragon Vo agon Win and Net 28064, 9150, M9607, M9650, QCA6174 CA8081 9379, Q0 2/SD 20 2/SD 20 2/SD 20 50 430, SI 0, SD 625 0, SD 625 0, SD 820 SD 845 / DM660, S	auror securi bullet	ity-			
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2299 Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301				w.cod ra.org rity- bullet	a- ity-	0-QUA- MSM8- 130819	
Out-of-	25-07-2019	7.5	Out of	bound a	ccess wł	nen	https:	//ww	0-QUA-	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 456	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
bounds Read			the frame length innSnapdragon Auto, SnapdragoniConsumer ElectronicsiConnectivity, SnapdragonjConsumer IOT, SnapdragoniIndustrial IOT, SnapdragoniMobile, Snapdragon Voice &iMusic in MDM9150,iMDM9206, MDM9607,iMDM9640, MDM9650,iMSM8996AU, QCA6174A,iQCA6574AU, QCA9377,iQCA9379, QCS405, QCS605, SDi425, SD 427, SD 430, SD 435,iSD 450, SD 625, SD 636, SDi665, SD 675, SD 712 / SD 710 /iSD 670, SD 730, SD 820, SDi820A, SD 835, SD 845 / SDi850, SD 855, SDA660, SDM630,iSDM660, SDX20, SDX24iCVE ID : CVE-2019-2305Improper casting of structure					leauro g/secu in/20 7/01/ 019- a- ity- in	MSM8- 130819	/869
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6					w.cod ra.org rity-	019- a- ity-	0-QUA- MSM8- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MSM8- 130819/871
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019-	O-QUA- MSM8- 130819/872
CV Scoring So (CVSS)	cale 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	n & CVE	ID	Pa	tch	NCIIP	CID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308 While storing calibrated data from firmware in cache. An				code- auror securi bullet	ity-		
Out-of- bounds Read	25-07-2019	7.5	CVE ID : CVE-2019-2308			w.cod ra.org rity-	in/20 7/01/ 019- a- ity-	0-QUA- MSM8- 130819		
mproper	25-07-2019	4.6	When handling the vendor			dor	https:	//ww	0-QUA-	
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3	3-4 459	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patc	h	NCIIP	C ID
Restriction of Operations within the Bounds of a Memory Buffer			command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	w.codea ra.org/s rity- bulletin 19/07/ july-20 code- aurora- security bulletin	secu 1/20 /01/ 19- y-	MSM8- 130819	/874
sd_410_firm	iware						
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655,	https:// w.qualc m.com/ mpany/ duct- security ulletins	com /co /pro y/b	0-QUA- 130819	
CV Scoring S	cale 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	4-5	5-6	6-7	7-8	8-9
				460					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2235		
			Null pointer dereference during secure application termination using specific		
NULL Pointer Dereferenc e	25-07-2019	2.1	application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/876

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				461						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2236		
N/A	25-07-2019	2.1	Failure in taking appropria action to handle the error of If keypad gpio deactivation fails leads to silent failure scenario and subsequent lo gets executed everytime in Snapdragon Auto, Snapdra Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / S 710 / SD 670, SD 730, SD 8 SXR1130	sase https://ww gon https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/877
Out-of- bounds Read	25-07-2019	4.6	CVE ID : CVE-2019-2237 Lack of check of data type of lead to subsequent loop- expression potentially go negative and the condition still evaluate to true leadin buffer underflow. in Snapdragon Auto, Snapdra Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / S 710 / SD 670, SD 730, SD 8 SXR1130	will g to gon https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/878
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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-2019-2238		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/879
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour	https://ww w.qualcom m.com/co mpany/pro duct- security/b	O-QUA-SD_4- 130819/880
CV Scoring St					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
462										

L

Weakness	Publ	ish Date	CVSS	I	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
				Description & CVE ID in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9605, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130					ns		
sd 412 firm	ware			CVE ID) : CVE-2	2019-22	41				
sd_412_firm Improper Restriction of Operations within the Bounds of a Memory Buffer	tion ons the of consectivity, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	—			
CV Scoring Scale (CVSS) 0-1		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2235		
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 632, SD 636, SD 650/52, SD 635, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/882
CV Scoring So	cale 0-1	1-2	2-3 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	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/883	
Out-of- bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2238	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/884	
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIP	PC ID
Improper Input Validation	25-07-2019	2.1	layout Corrup Denial Snapdr Compu Connec Consur Industr Mobile Music, Infrastr in MDM MDM90 MDM90 MDM90 QCS404 215, SE SD 410 430, SE SD 450 625, SE 650/52 710 / S SD 820 850, SE SDM43 SDX20, Snapdr SXR113	49150, N 607, MD 640, MD 655, MS 4, QCS60 0 210/SI /12, SD 0 435, SI 0 435, SI 0 632, SI 2, SD 675 30 670, S 0 670, S 0 670, S 0 8CX, SI 39, SDM6 , SDX24, ragon_Hi	an lead t can lead ce in ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra agon Vo agon Wir and Netw 4DM920 M9635N M9650, M8996A 05, Qualo 0 212/SI 425, SD 0 439 / S 5/16/SD 0 439 / S 5/16/SD 0 5, SD 712 SD 730, S S 5, SD 84 0 5, SD 84	ao SUI to odragon gon agon agon agon agon agon agon def working 06, 4, 40, 40, 40, 40, 415, SD 50 429, 415, SD 50 429, 415, SD 2 / SD 50 820, 45 / SD 4660, 2016,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
		7-2019 2.1	backgr	renderin ound, Er s not cau	ror stat	us	w.qua			
Improper Input Validation	25-07-2019		and als handlir to unin in Snap	o incorr ng is bein tended S odragon ragon Co	ect statu ng done SUI beha Auto,	ıs leading	m.com/co mpany/pro duct- security/b ulletins		0-QUA-SD_4- 130819/886	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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 C Image: Comparison of the second secon			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2241		
sd_820a_fir	mware				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/887
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 468	6-7 7-8	8-9 9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
468										

Weakness	Publi	ish Date	CVSS	C	escriptio	on & CVE	ID	Pat	ch	NCIIP	CID
				SD 450 636, SD SD 820 845 / S SDM43	, SD 625) 712 / S , SD 820 D 850, S 9, SDM6 agon_Hi	A, SD 83	2, SD SD 670, 35, SD SDA660, 4660,				
				CVE ID	: CVE-2	019-22	35				
NULL Pointer Dereferenc e	25-07	7-2019	2.1	during termina applica Auto, S Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA Snapdr SNA SNA SNA SNA SNA SNA SNA SNA SNA SNA	secure a ation us tion ids. napdrag agon Co agon Co agon Co agon Co agon Ma agon Ma agon Wa cucture a 074, MI 607, MD 655, MS 81, QCS 0 410/12 0 430, SI 0 430, SI 0 430, SI 0 55, SD 81, QCS 0 410/12 0 430, SI 0 55, MS 81, QCS 0 410/12 0 430, SI 0 55, MS 81, QCS 0 410/12 0 430, SI 0 430, SI 0 50 450 0 636, SI 0 712 / S 30	vice & M ired and Net DM9206 M9650, M8996A 605, Qua 2, SD 42 D 435, SI 0, SD 625 D 650/5 SD 710 / 0, SD 820	on ific odragon pute, ity, ity, IOT, IOT, USIC, usic, working , U, alcomm 5, SD 2, SD 2, SD 2, SD 2, SD 5, SD 2, SD 3, SD 2, SD 439 / 5, SD 2, SD 3, SD 439 / 5, SD 2, SD 439 / 5, SD 2, SD 439 / 5, SD 2, SD 439 / 5, SD 2, SD 3, SD 4, SD 4, SD	https:, w.qua m.com mpany duct- securi ulletin	lcom 1/co y/pro ty/b	0-QUA- 130819	
Improper Input	25-07	7-2019	2.1	Sanity checks are missing in layout which can lead to SUI			https: w.qua	-	0-QUA- 130819		
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descripti	on & CVE ID		Pat	tch	NCIIP	CID
Validation			Corruption or Denial of Servi Snapdragon Au Compute, Snap Connectivity, S Consumer Elec Connectivity, S Consumer IOT Industrial IOT, Mobile, Snapdra Infrastructure in MDM9150, I MDM9607, ME MDM9640, ME MDM9655, MS QCS404, QCS6 215, SD 210/S SD 410/12, SD 430, SD 435, S SD 450, SD 632, S SD 450, SD 632, S 650/52, SD 632, S 650/52, SD 632, S 650/52, SD 632, S SD 820A, SD 83 850, SD 8CX, S SDM439, SDM4 SDX20, SDX24 Snapdragon_H SXR1130 CVE ID : CVE-2	ce in uto, Snapdr odragon Snapdragon Snapdragon Snapdragon , Snapdrago ragon Voice agon Wired and Netwo MDM9206, 0M9635M, 0M9635M, 0M9650, SM8996AU, 05, Qualcon D 212/SD 2 425, SD 42 D 439 / SD 5/16/SD 41 D 636, SD 5, SD 712 / SD 730, SD 35, SD 845 DA660, 630, SDM66 , igh_Med_20	ragon i on e & l orking 205, 27, SD 429, 15, SD 820, / SD 820, / SD 820, / SD 820, / SD 60, 016,	m.con mpany duct- securi ulletir	y/pro ity/b		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon			https: w.qua m.con mpany duct- securi ulletir	n/co y/pro ity/b	0-QUA- 130819	
	ale o t								

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-0UA-SD 8-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	CVE ID : CVE-2019-2241 Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/892
Improper Input	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a	https://ww w.qualcom	0-QUA-SD_8- 130819/893
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 472	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	C ID
Validation			Snapdr Connec Consum Industr IoT, Sna Snapdr Snapdr MDM92 MDM92 MSM89 QCS405 215, SD SD 425 435, SD SD 425 435, SD SD 600 625, SD SD 675 670, SD SD 835 855, SD SDM63	ted comm ragon Au ctivity, Sr ner IOT, rial IOT, S apdragon ragon Vo ragon Vo ragon We 150, MD 607, SD 607, SD	ito, Snap napdrag Snapdra Snapdra n Mobile ice & Mu earables M9206, M9650, SM8996 05, Qualc 0 212/SI 7, SD 430 SD 429, S /16/SD 0 636, SI 2 / SD 71 0 820, SI 5 / SD 85 DM439, 560, SDX	odragon agon agon e, usic, s in 5AU, comm D 205, 0, SD 5D 450, 415, SD 5D 450, 415, SD 5D 665, 0 / SD 5D 820A, 50, SD	m.con mpan duct- securi ulletin	y/pro ity/b		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9625, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/895
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other	https://ww w.qualcom	0-QUA-SD_8- 130819/896
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	De	escription	n & CVE I	D	Pa	tch	NCIIP	C ID
			non secu can lead disclosur Snapdrag Snapdrag Snapdrag Snapdrag Snapdrag Snapdrag Snapdrag Infrastru in IPQ80 MDM965 QCA8082 215, SD 2 SD 425, S 435, SD 4 SD 625, S 650/52, 710 / SD SD 820A 850, SD 8 SDM439 Snapdrag SXR1130 CVE ID :	to infor re in Sna gon Com gon Com gon Com gon Ind gon Mol gon Voie gon Wir acture an 074, MD 06, MD 50, MSM 1, QCS66 210/SD 50, MSM 1, QCS66 210/SD SD 427, 439 / SI SD 632, SD 632, SD 632, SD 632, SD 635, SD 0 670, SI 5, SD 835 855, SD 5, SDM63 gon_Hig 0	rmation apdrage npute, nectivi nsumer ustrial bile, ce & Mu red nd Netw M9150, 49607, 18996A 05, Qua 212/SI SD 430 D 429, S SD 636 , SD 712 D 730, S SD 636 , SD 712 D 730, S SJ 84 8CX, SI 30, SDM gh_Med	on Auto, ty, IOT, IOT, Isic, working U, Icomm D 205, , SD 5D 450, , SD 2 / SD 5D 820, 5 / SD	m.com mpan duct- secur ulletin	y/pro ity/b		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650,			w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
			1	10, 1101	1,000)					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263		
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/898
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/899
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130		
			CVE ID : CVE-2019-2269		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/900
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/901
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24		
			CVE ID : CVE-2019-2276		
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/902
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/903
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Dat	e CVSS	Descripti	on & CVE ID	P	atch	NCIIF	'C ID
			215, SD 210/S SD 425, SD 439 450, SD 625, S SD 665, SD 679 710 / SD 670, S SD 820A, SD 83 850, SD 855, S SDM630, SDM6 SDX24, Snapdragon_H CVE ID : CVE-2	9 / SD 429, S D 632, SD 63 5, SD 712 / S SD 730, SD 8 35, SD 845 / DA660, SDM 660, SDX20,	D 6, D 20, SD 439,			
NULL Pointer Dereferenc e	25-07-201	9 7.8	Null pointer de happen when y with wrong blo Snapdragon Au Compute, Snap Consumer IOT Industrial IOT, IoT, Snapdragon Vo Snapdragon Vo Snapdragon W MDM9150, ME MDM9607, ME MDM9607, ME MDM9607, ME MSM8909W, M QCS405, QCS6 215, SD 210/S SD 425, SD 427 435, SD 439 / 3 SD 600, SD 615 625, SD 632, S SD 675, SD 717 670, SD 730, S SD 835, SD 845 SD 835, SD 845 SDM630, SDM0 Snapdragon_H CVE ID : CVE-2	playing the c ock group id uto, Snapdra odragon , Snapdragon , Snapdragon on Mobile, oice & Music Vearables in DM9206, DM9650, ASM8996AU, 05, Qualcom D 212/SD 20 7, SD 430, SD SD 429, SD 4 5/16/SD 415 D 636, SD 66 2 / SD 710 / D 820, SD 82 5 / SD 850, S SDM439, 660, SDX20, igh_Med_20	lip in gon n , , , , , , , , , , , , , , , , , ,	rity/b	0-QUA- 130819	
Improper Restriction of	25-07-201	9 2.1	Out of bound r information di	sclosure in	w.qu	s://ww alcom m/co	0-QUA- 130819	
			III III ware uue	firmware due to insufficient				
CV Scoring Sc								

Weakness	Publish Date	CVSS	De	escriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
Operations within the Bounds of a Memory Buffer			checking structur a kernel Auto, Sn Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra MSM890 QCS605, 210/SD SD 427, 439 / SE SD 632, 675, SD SD 730, 835, SD SD 8CX, SDM630 Snapdra SXR1130	re that c driver apdrag agon Co agon Co agon Co agon Mo agon Wo 09W, M , Qualco 212/SI SD 430 0 429, S SD 430 0 429, S SD 636 712 / S SD 820 845 / S SDA66 0, SDM6 agon_Hi 0	an be se in Snape on Com nnectivi nsumer dustrial obile, ice & Mu earables SM8996 omm 21 0 205, Sl o 205, Sl o 205, Sl o 450, S D 450, S D 450, S D 710 / SD 820 S 850, S 0, SDM4 o60, gh_Med	ent from dragon pute, ty, IOT, IOT, IOT, SD 625, SD 625, SD 625, SD 670, A, SD SD 670, A, SD SD 855, 39, _2016,	mpan duct- securi ulletin			
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2345				w.cod ra.org rity- bullet 19/07 july-2 code- auror securi bullet	7/01/ 019- a- ity- in	0-QUA- 130819	/906
Out-of-	22-07-2019	7.5	Imprope	er valid	ation for	r inputs	https:	//ww	O-QUA-	SD_8-
CV Scoring Sc. (CVSS)	ale 0-1	1-2	2-3	3-4 480	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pa	tch	NCIIP	C ID
bounds Write			Comput Consum Industr Mobile, Music, S in MDM MDM96 MDM96 MDM96 MSM89 QCS405 215, SD SD 425, 435, SD SD 425, 435, SD SD 625, 665, SD SD 625, 665, SD SD 670, 820A, S 850, SD SDM630 SDX24	an out o video d agon Au te, Snapo ner IOT, ial IOT, s Snapdra (9150, M 507, MD) 507, MD 507, MD) 507, MD 507, MD 50	f bound river. in to, Snap dragon Snapdra agon Vo gon We 1DM920 M9640, M8909V (CA6574 (5, Qualc (5, Qualc	write odragon agon ice & arables 06, V, 4AU, comm D 205, 0, SD SD 450, 5, SD SD 710 / 0, SD SD 710 / 0, SD 205, 30 SD 710 / 0, SD 20, 30 20, 3	ra.org rity-	2019- a- ity-	130819	/907
Use After Free	25-07-2019	4.6	multiple camera destroy in Snapdra Snapdra Snapdra Snapdra Snapdra MDM92 MDM96 MSM89	driver t red sessi dragon Co agon Co agon Inc agon Mc agon We 206, MD 540, MD 540, MD	ls will le to access on data Auto, nnectivi nsumer dustrial obile, earables M9607, M9650, SM8996	ad pointer ity, IOT, IOT, in	w.cod ra.org rity-	019- a- ity-	0-QUA- 130819	
			QCS605 430, SD SD 636,		9 450, SI	0 625,				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_8- 130819/909
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_8- 130819/910
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2298		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/911
Improper Restriction of Operations within the Bounds of	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20	0-QUA-SD_8- 130819/912
CV Scoring So (CVSS)	cale 0-1	1-2	Consumer IOT, Snapdragon 2-3 3-4 4-5 5-6 483	19/07/01/ 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24	july-2019- code- aurora- security- bulletin	
Out-of- bounds Read	25-07-2019	7.5	CVE ID : CVE-2019-2301 Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/913
Improper Restriction of	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display	https://ww w.codeauro ra.org/secu	0-QUA-SD_8- 130819/914
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 484	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
Operations within the Bounds of a Memory Buffer			Snapdr Snapdr Snapdr Snapdr Mobile, Music, S in MDM MDM96 MSM89 QCS405 215, SD SD 425 435, SD SD 425 435, SD SD 615 632, SD SD 712 730, SD SD 845 SDA660 SDM66	odragon Co ragon Co ragon Co ragon Ind ragon Ind ragon Io ragon Io ra ragon Io ra ragon Io ra ragon Io ra ragon Io ra ragon Io ragon Io ra	nnectivi nsumer dustrial F, Snapd agon Vo gon We ADM920 M9650, (SM8996 D5, Qualc D5, Qualc D5, Qualc D5, Qualc D5, Qualc D5, Qualc D5, Qualc D5, Qualc D65, SI 0429, S 415, SD D665, SI 0/SD 65 S106 D820A, S 0, SD 85 39, SDM 0	IOT, IOT, Iragon bice & arables 06, 5AU, comm D 205, 0, SD 5D 450, 625, SD 5D 450, 625, SD 5D 675, 570, SD SD 835, 55, 1630,		a- ity-		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	due to l calculat 802.11 configu Auto, Si Electro Snapdr Snapdr Snapdr Snapdr MDM96 MDM96 QCA61 QCA93 QCS605 205, SD	le integen lack of va tion of d Rx mana tration in napdrag onics Con ragon Co ragon Co ragon Mo ragon Mo 150, MD 607, MD 607, MD 650, MS 74A, QC 77, QCA 5, SD 210	alidation agemen n Snapdi on Cons nectivit nsumer dustrial obile, nice & Mu M9206, M9640, M9640, M8996A A6574A 9379, Q0	n before th in t ragon sumer ty, IOT, IOT, usic in U, U, CS405, 2/SD D 430,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_
			30 433	, 30 430	, 50 000	עט,י		1	1	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2307		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/916
			While storing calibrated data	https://ww	
Out-of- bounds Read	25-07-2019	7.5	from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-	0-QUA-SD_8- 130819/917
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2309	security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/918
	215_firmware				
Improper Restriction	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to	https://ww w.qualcom	0-QUA-QUAL-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 487	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	escription & C	CVE ID	Ра	tch	NCIIP	CID
of Operations within the Bounds of a Memory Buffer			TA rollb Snapdra Comput Connect Consum Industri Mobile, Music, S Infrastr in MDM MDM96 MSM89 QCS605 410/12 430, SD SD 450, 636, SD SD 820, 845 / SI SDM439 Snapdra SXR113	ize assumpt back protect agon Auto, S agon Auto, S agon Auto, S agon Auto, S agon Auto, S agon, SD agon_High_M o ack protection agon_High_M o ack protection agon_High_M o ack protection agon_High_M o ack protection agon_High_M o	ion logic. in napdragon on ragon cs ragon odragon odragon dvoice & Wired Vetworking 9607, 55, 04, 215, SD 427, SD 427, SD 0 / SD 429, 632, SD 0 / SD 670, 0 835, SD 2X, SDA660, 1ed_2016,	m.cor mpan duct- secur ulletin	y/pro ity/b	130819	/919
NULL Pointer Dereferenc e	25-07-2019	2.1	Null poi during s termina applicat Auto, Sr Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra infrastr in IPQ80	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	-		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 4-5	5 5-6	6-7	7-8	8-9	9-10

Improper Input ValidationZ5-07-2019Z.1MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 429, SD 420, SD 820, SD 820, SD 835, SD 8CX, SD A660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130Ktps://ww wt.qualcom nt.com/co mpany/pro duct.Improper Input ValidationZ5-07-2019Z.1Sanity checks are missing in Infrastructure and Networking in MDM9150, MDM9206, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 212/SD 225, SD 430, SD 845, SD 439 / SD 430, SD 435, SD 439 / SD 439, SD 430, SD 435, SD 439 / SD 430, SD 435, SD 430 / SD 430, SD 430, SD 345, SDImproper MDM9652, M3 9 / SD 430 / SD 435 / SD 140 / 20, SD 430 / SD 435 / SD 430 / SD 430, SD 435, SD 430 / SD 430 / SD 430, SD 435, SD 430 / SD 430 / SD 430, SD 435, SD 430 / SD 430 / SD 430 / SD 435 / SD 140 / 20, SD 635 / SD 630 /	Weakness	Publish Date	CVSS	[Descriptic	on & CVE	ID	Pa	tch	NCIIP	PC ID
Improper Input ValidationIayout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, SnapdragonIndustrial Mobile, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Noice & Music, Snapdragon Noice & MDM96150, MDM9206, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 650/52, SD 675, SD 712 / SD SD 820A, SD 835, SD 845 / SD0-QUA O-QUA- O-Q				MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236							
CV Scoring Scale	Input	25-07-2019	2.1	layout Corrup Denial Snapdn Compu Connec Consur Industr Mobile Music, Infrast in MDM MDM9 MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52 710 / S	which ca of Service ragon Au reagon Au rete, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, , Snapdra ructure a A9150, M 607, MD 640, MD 640, MD 655, MS 4, QCS60 0 210/SI 0/12, SD 0 435, SI 0, SD 615 0 632, SI 2, SD 679, S	an lead t can lead ce in ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra Snapdra and Net ADM920 M96351 M96350, M8996A D5, Qual D 212/S 425, SD D 439 / S 5/16/SD D 636, SI 5, SD 71	to SUI to odragon gon gon agon agon agon agon agon de ced working 06, M, U, comm D 205, 427, SD SD 429, 415, SD D 2 / SD SD 820,	w.qua m.cor mpan duct- secur	alcom n/co y/pro ity/b		
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	-	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2239		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Vearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-QUAL- 130819/922
			CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-QUAL- 130819/923
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch		NCIIP	CID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254				
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD	https://www.codeau ra.org/se rity- bulletin/ 19/06/0 june-201 code- aurora- security- bulletin	uro ecu /20)3/ 19-	0-QUA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 491	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QUAL- 130819/925
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct-	0-QUA-QUAL- 130819/926
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 492	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273	security/b ulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-QUAL- 130819/927

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				493						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016		
			CVE ID : CVE-2019-2279		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-QUAL- 130819/928
			CVE ID : CVE-2019-2334 Out of bound read and		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QUAL- 130819/929
CV Scoring So (CVSS)	cale 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	on & CVE	ID	Ра	tch	NCIIP	CID
			MSM8 ⁴ QCS60 210/SI SD 427 439 / S SD 632 675, SI SD 730 835, SI SD 8CX SDM63), SD 820 D 845 / S X, SDA66 80, SDM6 ragon_H	ISM8996 omm 21 D 205, S O, SD 435 SD 450, S SD 450, S SD 710 / O, SD 820 SD 850, S O, SDM4 560,	6AU, 5, SD D 425, 5, SD SD 625, 5, SD 7 SD 670, 0A, SD SD 855, 139,				
			CVE ID) : CVE-2	2019-23	43				
Out-of- bounds Write	22-07-2019	7.5	receive lead to issue in Snapdu Compu Consur Indust Mobile Music, in MDM MDM9 MDM9 MSM89 QCS40 215, SI SD 425 435, SI SD 625 665, SI SD 670 820A, SI	CVE ID : CVE-2019-2343 Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,				//ww leauro g/secu in/20 6/03/ 2019- a- ity- in	0-QUA- 130819	
CV Scoring Sc	cale 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
			CVE ID : CVE-2019-2287		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-QUAL- 130819/931
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-QUAL- 130819/932
	cale		SD 712 / SD 710 / SD 670, SD		

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				496						

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Ра	tch	NCIIP	CID
			730, SD SD 845 SDA660 SDM660	/ SD 85), SDM4), SDX2	0, SD 85 39, SDM 0					
			CVE ID	06						
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308		w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	-		
sd_205_firm	iware									
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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 in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237		
Out-of- bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2238	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/935
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/936
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 498	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	PC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9635M, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239				
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150,	https:/ w.qual m.com mpany duct- securit ulletin	lcom 1/co 7/pro ty/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIP	CID
			MDM92 MDM94 MSM89 QCA65 QCA65 QCA65 QCA93 QCA98 QCA98 QCA98 QCN55 SD 210 425, SI SD 210 425, SI SD 675 670, SI SD 835 855, SI SDM63 SDX24, CVE ID							
Improper Input Validation	25-07-2019	2.1	CVE ID : CVE-2019-2240While rendering the layoutbackground, Error statuscheck is not caught properlyand also incorrect statushandling is being done leadingto unintended SUI behaviourin Snapdragon Auto,Snapdragon Compute,Snapdragon Connectivity,Snapdragon ConsumerElectronics Connectivity,Snapdragon Industrial IOT,Snapdragon Mobile,Snapdragon WiredInfrastructure and Networkingin MDM9150, MDM9206,MDM9655, MSM8996AU,QCS404, QCS605, SD 210/SD212/SD 205, SD 410/12, SD636, SD 675, SD 712 / SD 710 /				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130		
			CVE ID : CVE-2019-2241		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/939
			CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/940
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID			Pa	tch	NCIIPC ID		
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253							
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX,			https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins		0-QUA-SD_2- 130819/941		
			SDA66	0, SDM4		1630.				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130				
			CVE ID : CVE-2019-2254				
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_2- 130819/942		
			CVE ID : CVE-2019-2260				
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/943		
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 503	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID			Pa	tch	NCIIPC ID		
			Description & CVL ID Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130							
Use After Free	25-07-2019	4.6 A ha di fr Si Si Si Si Si M M M M M M M M M M M M M	CVE ID : CVE-2019-2261 Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660,				https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin		0-QUA-SD_2- 130819/944	

Weakness	Publish Date	CVSS	•					tch	NCIIP	CID
			•	, ragon_Hi) : CVE-2	0 -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer display validat set by t Auto, S IOT, Sr IOT, Sr IOT, Sr Snapdu Snapdu Snapdu MDM9 MDM9 MSM89 212/SI SD 430 615/10 636, SI	cur in o lack of ock size gon sumer strial usic, s in V, SD D 427, D 427, D 427, D 5, SD 2 / SD 2 / SD , SD 845 (20)	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819			
Out-of- bounds Read	25-07-2019	7.8	playing denial Snapdu Compu Conneu Consuu Industu Mobile Music, in MSM Qualco 212/SI SD 430 429, SI 650/52	e issue i ito, Snap dragon napdrag Snapdra Snapdra agon Ve gon We , QCS60 5, SD 210 5, SD 210 5, SD 439 5, SD 439 5, SD 67	e leads to in odragon agon agon oice & arables 5, 0/SD D 427, 0 / SD D	https w.qua m.cor	y/pro ity/b	0-QUA- 130819		
CV Scoring So (CVSS)	cale 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	on & CVE	Ра	tch	NCIIP	C ID	
			855, SI), SD 845) 8CX, SI [.] agon_Hi 30	DM439,					
			CVE ID) : CVE-2	019-22	73				
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277					//ww eauro g/secu in/20 5/03/ 2019- a- ity- in	0-QUA- 130819	_
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	with in to acce memor Snapdr Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 MSM8 ⁴ QCS40 215, SI	nd the al apdrago onnectiv onsumer dustrial	hay lead located n Auto, ity, IOT, IOT, usic, s in V, 4AU, comm D 205,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016		
			CVE ID : CVE-2019-2279		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/949
Improper Restriction of Operations within the	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from	https://ww w.qualcom m.com/co mpany/pro duct-	0-QUA-SD_2- 130819/950
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670 SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343	, security/b ulletins	
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD		0-QUA-SD_2- 130819/951
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2287		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_2- 130819/952
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/953
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2298		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_2- 130819/954
Improper Restriction of Operations	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto,	https://ww w.codeauro ra.org/secu rity-	0-QUA-SD_2- 130819/955
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 510	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pa	tch	NCIIP	C ID
within the Bounds of a Memory Buffer			Snapdr Snapdr Snapdr Snapdr Mobile Music, in MDM MDM99 MSM89 QCS409 215, SI SD 425 435, SI SD 425 435, SI SD 615 632, SI SD 712 730, SI SD 712 730, SI SD 845 SDA66 SDM66	bullet 19/07 july-2 code- auror secur bullet	019- a- ity-					
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	CVE ID : CVE-2019-2306 Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2307		
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_2- 130819/957
			CVE ID : CVE-2019-2309		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_2- 130819/958
CV Scoring S (CVSS)	cale 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	Pa	tch	NCIIP	C ID	
			QCA61 QCA93 QCS60 205, SI SD 435 625, SI SD 712 730, SI SD 845 SDM63	640, MS 74A, QC 77, QCA 5, SD 21 0 425, SI 0 425, SI 5, SD 450 0 636, SI 2 / SD 71 0 820, SI 5 / SD 85 80, SDM6	A6574A 9379, Q 0/SD 21 0 427, S 0, SD 600 0 665, S 0 665, S 0 / SD 6 0 820A, 50, SD 85 560, SDX					
sd_210_firm	iware		CVE ID : CVE-2019-2312							
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
Out-of- bounds Read	25-07-2019	4.6	lead to exprest negativ still eva buffer	o true lea ow. in	p-	w.qua m.cor	n/co y/pro	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	•				Pa	tch	NCIIP	CID
			Consum Connect Consum Industr Mobile MDM90 210/SI 410/12	te, Snap ner Elect ctivity, Si ner IOT, rial IOT, in MDM 607, MD 655, QCS 0 212/SI 2, SD 679 SD 670, S 30	tronics napdrag Snapdra 9206, M9650, S605, SD 5, SD 711	ulletii	ns			
			CVE ID : CVE-2019-2238							
Improper Input Validation	25-07-2019	2.1	layout y Corrup Denial Snapdr Compu Connec Consum Industr Mobile, Music, y Infrastr in MDM MDM90 MDM90 QCS404 215, SE SD 410 430, SE SD 450 625, SE 650/52 710 / S SD 820	49150, M 607, MD 640, MD 655, MSI 4, QCS60 210/SI /12, SD 0 435, SE	an lead t can lead ce in to, Snap dragon napdrag tronics napdrag Snapdra Snapdra gon Win and Net 1DM920 M9635N M9650, M8996A 05, Qualo 0 212/S 425, SD 0 439 / S /16/SD 0 636, SI 5, SD 71 5, SD 84	a SUI to odragon gon gon agon agon agon agon agon ag	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So	cale 0-1	1-2	2-3	3-4	0A660, 4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0-1	12	23	514		50	07	7.0	0.5	5 10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSS	SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239 While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,		NCIIPC ID
N/A	25-07-2019	2.1	Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/962
			855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130		

CV Scoring Scale (CVSS)

2-3

6-7

Weakness	Publi	sh Date	CVSS	ſ	Description & CVE ID			Pa	tch	NCIIP	CID
				CVE ID : CVE-2019-2240							
Improper Input Validation	25-07	7-2019	2.1	backgr check i and als handlin to unin in Snapdn Sn	itended i odragon Co ragon Co ragon Co ragon Co ragon Co ragon In ragon Mo ragon W ructure A9150, N 607, MD 655, MS 4, QCS60 0 205, SI 0 675, SI 0 675, SI 0 835, SI 60, SDM6	ror stat aght pro ect statung done SUI beha Auto, mpute, mnectivit mectivi mectivi mectivi mectivit mectivit mectivit mectivit me	us perly is leading aviour ity, ty, IOT, IOT, IOT, IOT, IOT, SD 2, SD 2, SD 5D 710 / 0, SD 7 SD DA660, 524,	w.qua m.con mpan duct- secur ulletin	n/co y/pro ity/b	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07	7-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring Sc (CVSS)	ale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9
				516					

Weakness	Publish Date	CVSS	Description & CVE ID			ID	Pa	tch	NCIIF	PC ID
			MDM9 MSM89 210/SI SD 427 439 / S 615/16 632, SI SD 712 730, SI SD 845 SDA66 SDM66	49206, M 650, MS 996AU, (0 212/S 7, SD 430 5D 429, S 6/SD 41 0 636, SI 2 / SD 71 0 820, SI 5 / SD 85 0, SDM4 50 9 : CVE-2	M8909V (CS605, D 205, S SD 435 (5, SD 435 (5, SD 435 (5, SD 435 (5, SD 45 (665, SI (0 / SD 6 (0 820A, S (0, SD 85 (39, SDM)	V, SD D 425, 5, SD 5, SD 5, SD 0 675, 570, SD SD 835, 55, 1630,				
Improper Input Validation	25-07-2019	7.5	while p corrup Snapdr Connec Consur Industr IoT, Sn Snapdr MDM9 MDM9 MDM9 MSM89 QCS40 215, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63	ted com ragon Au ctivity, S ner IOT, rial IOT, apdrago ragon Vo ragon W 150, MD 607, MD 607, MD 607, MD 5, QCS60 0 210/SI 5, SD 427 0 439 / S	in ogg fil ment blo ito, Snap napdrag Snapdra Snapdra Snapdra in Mobil bice & Mi earables M9206, M9650, SM8996 D5, Qualo D5, Qualo D6, SD S0, SD S0, SD S0, SD	le with a ock. in odragon agon e, usic, s in 5AU, comm D 205, 0, SD 5D 450, 415, SD 5D 450, 415, SD 5D 665, .0 / SD 5D 820A, 50, SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
Informatio	25-07-2019	7.5	Position determination			https:	//ww	0-QUA-	SD_2-	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 517	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
n Exposure			to wron inform Auto, S Snapdr Snapdr Snapdr Mobile Music, in MDM MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9	GD 710 / SD 820 SD 850, S 0, SDM4 S0, SDX2 ragon_Hi 30	oded Snapdra gon Com nsumer dustrial F, Snapd agon Vo gon We 4DM920 M9615, M9650, M9650, M9650, M9650, M8909V QCS605, SD 210 O 425, SI 665, SD SD 670, SD 632, SI 665, SD SD 670, A, SD 83 SD 855, S 39, SDM 0, gh_Med	agon pute, IOT, IOT, Iragon ice & arables 06, 4, V, V, V, D/SD D 427, 0 / SD 0 427, 0 / SD 6 / SD 0 636, 675, SD 6 75, SD 50 8CX, 630, 2016,	w.qua m.cor mpan duct- secur ulletin	n/co y/pro ity/b	130819	/966
Use After Free	22-07-2019	6.9	CVE ID : CVE-2019-2254 A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,			w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	6	Descriptio	n & CVE	ID	Ра	tch	NCIIP	C ID
			QCS409 215, SE SD 425 435, SE SD 625 665, SE SD 730 845 / S SDM43 SDX20, Snapdr SXR113	650, MS 5, QCS60 5, QCS60 5, SD 427 5, SD 427 5, SD 632 5, SD 632 0, SD 820 50 850, S 69, SDM6 , SDX24, ragon_Hi 30 9 : CVE-2	05, Qualo 0 212/S 7, SD 430 5D 429, S 6, SD 636 5D 710 / A, SD 83 5D 855, 530, SDM gh_Med	comm D 205,), SD SD 450, 5, SD SD 670, 35, SD 4660, _2016,				
N/A	22-07-2019	4.9	subsyst non sec can lea disclos Snapdr SD 425 435, SE SD 625 650/52 710 / S SD 820 850, SE	approvided at term to H cure sub d to info ure in Sr cagon Co cagon Co cagon Co cagon Mo cagon Mo cagon Wi cagon Wi cagon Wi 206, MD 650, MSI 81, QCS6 0 210/SI 5, SD 427 0 439 / S 5, SD 632 2, SD 670, S 50 670, S 60, SD 83 0 855, SI 69, SDM6 cagon Hi	ILOS or of system is mapdrag mpute, nnectivit nsumer dustrial obile, ice & Mi ired and Network DM9150 M9607, M8996A 505, Qua 0 212/Si 5, SD 430 5, SD 430 5, SD 430 5, SD 711 50 730, S 55, SD 84 0 8CX, SI 530, SDM	other memory on Auto, ity, IOT, IOT, usic, working , U, alcomm D 205, 0, SD 5D 450, 5, SD 2 / SD 5D 820, 45 / SD DA660, 4660,	https: w.qua m.cor	ity/pro	0-QUA- 130819	-
			onapai	agon_m	gn_meu	_2010,				

Weakness	Publish Date	CVSS	0	on & CVE	ID	Pa	tch	NCIIF	PC ID	
			SXR113	30						
			CVE ID	: CVE-2	019-22	61				
Use After Free	25-07-2019	4.6	happer diag dr free iss Snapdr Snapdr Snapdr Snapdr Snapdr Infrastr in IPQ4 MDM92 MDM92 QCA95 210/SI SD 427 450, SI 650/52 670, SI SD 845 SDX20, Snapdr	ragon Co ragon Co ragon In ragon Mo ragon W ragon W ructure 206, MD 206, MD 206, MD 206, MD 209W, M 31, QCA 0 212/Si 3, SD 430 0 212/Si 2, SD 430 0 225, SI 2, SD 711 0 820, SI 7 SD 85	reading f e to use a apdrago onnectiv onsumer dustrial obile, earables ired and Net Q8064, M9607, M9650, SM8996 9980, SI D 205, S 0, SD 435 D 636, SI 2 / SD 7 D 820A, 50, SDM6	from after on Auto, ity, IOT, IOT, S, working 6AU, D 0 425, 5, SD D 10 / SD SD 835, 660, _2016	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	display validat set by u Auto, S IOT, Sn IOT, Sn Snapdr Snapdr Snapdr MDM92		n due to eader bl Snapdra son Cons on Indus on IoT, obile, bice & M earables M9607, M8909V	o lack of ock size gon sumer strial usic, s in V,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20		
			CVE ID : CVE-2019-2272		
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/971
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_2- 130819/972
CV Scoring Se (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24		
			CVE ID : CVE-2019-2277		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_2- 130819/973
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/974
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	C ID
			Snapdr Snapdr MDM9 MDM9 MSM89 QCS40 215, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63 Snapdr	apdrago agon Vo agon Wo 150, MD 607, MD 009W, M 5, QCS60 0 210/SI , SD 427 0 439 / S 0 439 / S 0 439 / S 0 439 / S 0 50 615 0 632, SI 0 730, SI 0 730, SI 0 720, SI 0	vice & M earables M9206, M9650, SM8996 5, Quale 2, SD 430 SD 429, S 5/16/SD 2, SD 429, S 5/16/SD 2, SD 71 2, SD 71 2, SD 71 2, SD 85 5, SD	usic, 5 in 5AU, comm D 205, 0, SD 5D 450, 415, SD D 665, 0 / SD D 820A, 50, SD 50, SD 50, SD 50, SD				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of l inform firmwa checkin structu a kerne Auto, S Snapdr SD 427 439 / S SD 632	bound re ation dis are due t ng of an ere that of el driver napdrag ragon Co ragon Co ragon Co ragon Mo ragon Mo ragon Wo 209W, M 5, Qualco 0 212/SI 7, SD 430 50 429, S , SD 636	ead and sclosure o insuffi embedd can be so in Snap gon Com onnectiv onsumer dustrial obile, ice & M earables SM8996 omm 21 D 205, S 0, SD 435 SD 450, S 5, SD 665 SD 710 / 0, SD 820	in icient ed ent from dragon pute, ity, IOT, IOT, IOT, USIC, SD 5, SD D 425, 5, SD SD 625, 5, SD SD 625, 5, SD SD 670, DA, SD	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2343		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_2- 130819/976
Improper			Out of bound access can occur	https://ww	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150,	w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora-	0-QUA-SD_2- 130819/977
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	security- bulletin	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/978
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code-	O-QUA-SD_2- 130819/979
CV Scoring S (CVSS)	cale 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	Ра	tch	NCIIP	CID
			Mobile Music, Infrast in IPQ4 IPQ807 MDM9 MDM9 MSM89 QCA65 QCA93 SD 210 425, SI SD 210 425, SI SD 450 636, SI SD 670 820A, S 850, SI SDX24	4019, IP(74, MDM 206, MD 640, MD 996AU, (74AU, Q 77, QCA 0/SD 212 0 427, SI 0, SD 600 0 675, SI 0, SD 730 SD 835, SI	agon Vc agon Wir and Net 28064, 9150, M9607, M9650, QCA617 CA8081 9379, Q 2/SD 20 2/SD 20 0 430, SI 0, SD 62 0, SD 62 0, SD 820 50 845 / DM660, 1	oice & red working 4A, 5, SD 0 435, 5, SD 5, SD SD 710 / 0, SD 7 D SDX20,	auror secur bullet	ity-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improp while h to out o in Snapdr Snapdr Snapdr Snapdr Mobile Music, in MDM MDM9 MSM89 QCS40 215, SI SD 425 435, SI SD 615 632, SI SD 712	Der casti nandling of bound odragon ragon Co ragon Co ragon Io' , Snapdr Snapdra /19150, M 607, MD 909W, M 5, QCS60 0 210/SI 5, SD 427 0 439 / S	ng of str the buff I read in Auto, I read in Auto, I snapc dustrial T, Snapc agon Vc agon Vc agon We ADM920 M9650, SM8996 D5, Qual D5, Qual D5, Qual D5, Qual D5, Qual D5, Qual D5, Qual D429, S A15, SD 0 4 SD 6	ructure fer leads display ity, IOT, IOT, Iragon bice & arables 06, 5AU, comm D 205, 0, SD SD 450, 625, SD D 675, 570, SD	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_2- 130819/981
			CVE ID : CVE-2019-2307		
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	0-QUA-SD_2- 130819/982
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2309	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_2- 130819/983
sd_212_firm	iware				
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation	https://ww w.qualcom m.com/co	0-QUA-SD_2- 130819/984
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 528	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237	mpany/pro duct- security/b ulletins	
Out-of- bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2238	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/985
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to	https://ww w.qualcom m.com/co	0-QUA-SD_2- 130819/986
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 529	6-7 7-8	8-9 9-10

Denial of Service inmpany/proSnapdragon Auto, Snapdragonduct-Compute, Snapdragonconsectivity, SnapdragonConsumer Electronicsconnectivity, SnapdragonConsumer IOT, SnapdragonilletinsConsumer IOT, Snapdragonindustrial IOT, SnapdragonMobile, Snapdragon Wiredinfrastructure and Networkingin MDM9150, MDM9206,MDM9607, MDM9635M,MDM9607, MDM9650, MDM9650, MDM9650, MSM8996AU,QCS404, QCS605, Qualcomm215, SD 210/SD 212/SD 205,SD 410/12, SD 425, SD 427, SD430, SD 435, SD 439 / SD 429,SD 450, SD 615/16/SD 415, SD625, SD 632, SD 632, SD 845 / SD650/52, SD 675, SD 712 / SD710 / SD 670, SD 730, SD 820,SD 820A, SD 845, SD 845 / SD850, SD 8CX, SDA660,SDM439, SDM630, SDM660,SDX20, SDX24,Snapdragon_High_Med_2016,SXR1130CVE ID : CVE-2019-2239While sending the renderedwhile sending the renderedsurface content to the screen,Error handling is not properlyhttps://www.qualcom	Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	PC ID
surface content to the screen, Error handling is not properly https://ww				Snapdr Compu Connec Consum Consum Industr Mobile, Music, S Infrastr in MDM MDM96 MDM96 MDM96 MDM96 MDM96 QCS404 215, SE SD 410 430, SE SD 410 430, SE SD 450 625, SE 650/52 710 / S SD 820 850, SE SDM43 SDX20, Snapdr SXR113	agon Au te, Snap ctivity, Si ner Elec ctivity, Si ner IOT, rial IOT, Snapdra ructure a 19150, M 607, MD 640, MD 655, MSI 4, QCS60 0 210/SI /12, SD 6435, SE /12, SD 6155 0 632, SE 2, SD 675 0 632, SE 2, SD 675 0 632, SE 2, SD 675 0 632, SE 2, SD 675 30 8CX, SI 9, SDM6 SDX24, ragon_Hi 30	ito, Snap dragon napdrag tronics napdrag Snapdra agon Vo gon Wir and Netv 4DM920 M9635N M9650, M9650, M9650, M9996A D5, Qualo D 212/Si 425, SD 0 439 / Si /16/SD D 636, SI 5, SD 712 Si SD 730, Si Si Si Si Si Si Si Si Si Si Si S	gon agon agon ice & red working 06, 4, U, Comm D 205, 427, SD SD 429, 415, SD SD 429, 415, SD D 2 / SD SD 820, 45 / SD 4660, _2016,	duct- secur	ity/b		
N/A 25-07-2019 2.1 Checked results in an m.com/co n/A 25-07-2019 2.1 Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Letins Consumer IOT, Snapdragon	N/A	25-07-2019	2.1	surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon			w.qua m.con mpan duct- secur	llcom n/co y/pro ity/b	-		
CV Scoring Scale	-	cale 0-1	1-2			-	-	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	Pa	tch	NCIIP	C ID	
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240							
Improper Input Validation	25-07-2019	2.1					w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
			-	_		working				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2241		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/989
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in	https://ww w.qualcom m.com/co	0-QUA-SD_2- 130819/990
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 532	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	CID
			Connec Consur Industr IoT, Sn Snapdr Snapdr MDM9 MDM9 MSM89 QCS409 215, SE SD 425 435, SE SD 600 625, SE SD 675 670, SE SD 835 855, SE SDM63	ato, Snap napdrag Snapdra Snapdra on Mobile oice & Mi earables M9206, M9650, ISM8996 D5, Quale D 212/SI 7, SD 430 SD 429, S S/16/SD D 636, SI 2 / SD 71 D 820, SI S / SD 85 SDM439, S60, SDX 2019-22	gon agon agon e, usic, s in 6AU, comm D 205, 0, SD SD 450, 415, SD D 665, 10 / SD D 820A, 50, SD	mpan duct- secur ulletin	• •			
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9635M, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD				w.qua m.con	ity/b	0-QUA- 130819	
CV Scoring Sc			/							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_2- 130819/992
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory	https://ww w.qualcom m.com/co	0-QUA-SD_2- 130819/993
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 534	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descriptio	on & CVE I	D	Pat	tch	NCIIP	C ID
			can lead to info disclosure in Si Snapdragon Co Snapdragon Co Snapdragon Co Snapdragon Mo Snapdragon Mo Snapdragon Wo Infrastructure in IPQ8074, MI MDM9206, MD MDM9650, MS QCA8081, QCS 215, SD 210/Si SD 425, SD 427 435, SD 439 / S SD 625, SD 632 650/52, SD 673 710 / SD 670, S SD 820A, SD 83 850, SD 855, SI SDM439, SDM6 Snapdragon_Hi SXR1130 CVE ID : CVE-2	ormation napdrago ompute, onnectivit onsumer l obile, oice & Mu Vired and Netw DM9150, OM9607, SM8996AI 605, Qual D 212/SD 7, SD 430, SD 429, S 2, SD 636, 5, SD 712 SD 730, S 35, SD 84 D 8CX, SD 630, SDM igh_Med_	on Auto, ty, IOT, OT, sic, sic, vorking U, lcomm 205, SD 0 450, SD 0 450, SD 2 / SD 0 820, 5 / SD 0 820, 5 / SD 0 860, 660, 2016,		y/pro ity/b		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU,			w.cod ra.org rity-	:019- a- ity-	0-QUA- 130819	
			MSM8909W, M	1SM8996.	AU,				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_2- 130819/995
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/996
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 536	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273		
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_2- 130819/997
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora-	0-QUA-SD_2- 130819/998
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279	security- bulletin	
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/999

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				538						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_2- 130819/1000
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_2- 130819/1001
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_2- 130819/1002
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcom m.com/co mpany/pro duct-	O-QUA-SD_2- 130819/1003
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298 An out-of-bound write can be				securi			
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out- trigger comma userspa Snapdr Consum Consum Industr Mobile, Music, S Infrastr in IPQ4 IPQ807 MDM92 MDM92 MDM92 MDM92 SD 210 425, SE SD 450 636, SE SD 670	of-boun ed by a s ind supp ace appl agon Au ner Elec ctivity, Si ner IOT, rial IOT, Snapdra cucture a c019, IPC 24, MDM 206, MD 206, SI 20, 212 20, 20	id write specially lied by a ication. ito, Snap tronics napdrag Snapdra Snapdra Snapdra Snapdra Snapdra (Snapdra Snapdra Snapdra (Snapdra Snapdra (Snapdra Snapdra Snapdra (Snapdra Snapdra (Snapdra Snapdra (Snapdra Snapdra (Snapdra Snapdra (Snapdra Snapdra (Snapdra Snapdra (Snapdra Snapdra (can be r-crafted a in odragon agon agon oice & red working 4A, , CS605, 5, SD 0 435, 5, SD 50 710 / 0, SD	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDM660, SDX20 SDX24),	
			CVE ID : CVE-2019-2299		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer lead to out of bound read in displa- in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearable in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205 SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450 SD 615/16/SD 415, SD 625, S 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SI 730, SD 820, SD 820A, SD 83 SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20	ds ay https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- bulletin 5D bulletin	0-QUA-SD_2- 130819/1005
			CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation befo calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206,	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	0-QUA-SD_2- 130819/1006
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307		
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2309	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_2- 130819/1007
Improper Restriction of Operations	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of	https://ww w.codeauro ra.org/secu rity-	0-QUA-SD_2- 130819/1008
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 543	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	
sd_415_firm	iware				
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_4- 130819/1009

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				544						

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIF	PC ID
			SD 410 430, SI SD 450 625, SI 650/52 710 / S SD 820 850, SI SDM43 SDX20, Snapdr SXR113	D 439 / 5 5/16/SD D 636, SI 5, SD 71 5 5, SD 730, 5 85, SD 84 DA660, 530, SDM	427, SD SD 429, 415, SD 2 / SD SD 820, 45 / SD 4660, _2016,					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	end of s getting lead to in Snap Snapdr Snapdr Snapdr Mobile Music, in MDM MSM89 210/SI SD 427 439 / S 615/16 632, SI SD 712 730, SI SD 845 SDA66 SDM66	iterating informa odragon cagon Co cagon Co cagon Ino cagon Io sagon Io sag	gloop wi sion info ation dis Auto, mpute, msumer dustrial F, Snapd agon Vo gon We ADM960 M8909V QCS605, D 205, S D 206,	o and closure. IOT, IOT, Iragon ice & arables 07, V, SD D 425, 5, SD D 425, 5, SD 5,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	_
Improper	25-07-2019	7.5		over-rea			https:	//ww	0-QUA-	SD_4-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 545	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pa	tch	NCIIP	C ID
Input Validation			corrupt Snapdr Connec Consum Industr IoT, Sna Snapdr Snapdr MDM92 MDM92 MDM96 MSM89 QCS405 215, SD SD 425 435, SD SD 600 625, SD SD 675 670, SD SD 835 855, SD SDM63	ted comi agon Au tivity, Si ner IOT, ial IOT, apdrago agon Vo agon Wo 3gon Wo 507, MD 507, MD 509W, M 5, QCS60 210/SI , SD 427 0439 / S	ment blo ato, Snap napdrag Snapdra Snapdra n Mobilo ice & Mu earables M9206, M9650, SM8996 5, Qualo 5, SD 430 5, SD 430 5, SD 430 5, SD 7,	dragon agon gon e, isic, in 5AU, comm 5 205, , SD 50 450, 415, SD 5 665, 0 / SD 5 820A, 0, SD 2 0	w.qua m.con mpan duct- secur ulletin	n/co y/pro ity/b	130819	/1011
Informatio n Exposure	25-07-2019	7.5	accurac to wron informa Auto, Si Snapdr Snapdr Snapdr Mobile, Music, S in MDM MDM96 MDM96 MDM96 MDM96	n detern cy may b agly deco ation in 3 napdrag agon Co agon Io7 agon Io7 Snapdra Snapdra 607, MD 625, MD 625, MD 655, MSI 996AU, Q mm 215	e degrad oded Snapdra on Com nsumer dustrial Γ, Snapd agon Vo gon Wea 1DM920 M9615, M9635N M9650, M8909W QCS605,	ded due gon pute, IOT, IOT, ragon ice & arables 6, 1,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Desc	ription & CVE	Pa	tch	NCIIP	CID	
			SD 430, SD 429, SD 45 415, SD 62 SD 650/52 712 / SD 7 SD 820, SD 845 / SD 8 SDA660, SI SDM660, S	5, SD 425, S 435, SD 439 0, SD 615/1 5, SD 632, S 5, SD 665, SD 10 / SD 670, 820A, SD 83 50, SD 855, S DM439, SDM DX20, n_High_Med	9 / SD 6/SD 0 636, 675, SD SD 730, 35, SD SD 8CX, 630,				
			CVE ID : C	VE-2019-22	54				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	display fun validation set by user Auto, Snap IOT, Snapd IOT, Snapd Snapdrago Snapdrago MDM9206 MDM9650 MDM9650 MSM89967 212/SD 20 SD 430, SD 615/16/SI 636, SD 65 710 / SD 6	0	lack of ock size gon sumer trial usic, in V, SD D 427, 0, SD 5, SD 2 / SD 5, SD 2 / SD 5, SD 2 / SD 5, SD	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointe happen wh with wrong Snapdrago Compute, S Consumer Industrial	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3	-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	0	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			Snapdr Snapdr MDM9 MDM9 QCS409 215, SE SD 425 435, SE SD 600 625, SE SD 675 670, SE SD 835 855, SE SDM63 Snapdr	apdrago ragon Vo ragon Wo 150, MD 607, MD 909W, M 5, QCS60 9 210/SI 6, SD 427 9 439 / S 9, SD 615 9 632, SE 6, SD 712 9 730, SE 5, SD 712 9 730, SE 5, SD 845 9 A660, S 60, SDM6 ragon_Hi 9 : CVE-2	ice & M earables M9206, M9650, SM8996 5, Qualo 212/S 5, Qualo 212/S 5, Qualo 212/S 5, Qualo 2429, S /16/SD 636, SI / SD 71 0 820, SI / SD 85 DM439, 560, SDX gh_Med	usic, in 5AU, comm D 205, 0, SD 5D 450, 415, SD D 665, 0 / SD D 820A, 50, SD 20, SD 20, 20, 2016				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	while h to out o in Snapdr Snapdr Snapdr Snapdr Snapdr Mobile Music, in MDM MDM90 QCS409 215, SE SD 425 435, SE SD 615 632, SE SD 712 730, SE	of bound odragon ragon Co ragon Co ragon Io ragon Io ragon Io ragon Io ragon Io ragon Io ragon M 5, SD 427 So 210/SI 5, SD 427 So 439 / S	the buff read in Auto, nnective nsumer dustrial f, Snapc agon Vo gon We 1DM920 M9650, SM8996 05, Qualo 05, Qualo 05, Qualo 05, Qualo 05, Qualo 0212/S 50 429, S 415, SD 0665, SI 0 420A, S	Fer leads display ity, IOT, IOT, IOT, ice & arables 06, 5AU, comm D 205, 0, SD 5D 450, 625, SD 0 675, 70, SD SD 835,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIF	PC ID
				0, SDM4 50, SDX2		1630,				
						06				
			CVEID) : CVE-2	019-23	06				
sd_425_firm	iware									
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	emulat sector : TA roll Snapdr Compu Consur Consur Industr Mobile Music, Infrastr in MDM MSM89 QCS609 410/12 430, SI SD 4500 636, SI SD 8200 845 / S SDM43 Snapdr SXR113 CVE ID	ragon Au ite, Snap ctivity, Si ner Elec ctivity, Si ner IOT, rial IOT, , Snapdr Snapdra ructure a 49206, M 650, MD 996AU, Q 5, Qualco 2, SD 425 0, SD 625 0, SD 625 0, SD 625 0, SD 820 SD 850, S 39, SDM6 ragon_Hi 30	B is used imption otection ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra agon Vo gon Win and Net 1DM960 M9655, QCS404, 0M9655, QCS404, 5, SD 42 0 439 / S 5, SD 42 0 710 / A, SD 83 50 8CX, S 50 8C	l due to s in the logic. in odragon gon agon agon ice & red working 07, 5, SD 7, SD 5, SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIF	PC ID
			Snapdr Snapdr Snapdr Snapdr Infrast in IPQ& MDM9 QCA80 215, SI 427, SI SD 429 632, SI 675, SI SD 730 835, SI SDM43	8074, MI 607, MD 655, MS 81, QCS 0 410/12 0 430, SI 0 430, SI 0 50 450 0 636, SI 0 712 / S 0 50 820 0 8CX, SI 89, SDM 6 ragon_Hi	dustrial obile, oice & M ired and Net OM9206 M9650, M8996A 605, Qua 2, SD 42 O 435, SI 0, SD 625 O 650/5 SD 710 / O, SD 820 OA660, 530, SDM	IOT, usic, working , AU, alcomm 5, SD D 439 / 5, SD 2, SD 2, SD 2, SD 3D 670,)A, SD				
Improper Input Validation	25-07-2019	2.1	Sanity layout Corrup Denial Snapdr Compu Connec Consur Consur Industr Mobile Music, Infrast in MDM MDM9 MDM9 QCS40	e: CVE-2 checks a which ca otion or o of Servio ragon Au te, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, , Snapdr Snapdra ructure 49150, M 607, MD 640, MD 655, MS 4, QCS60 0 210/SI	are missi an lead t can lead tc in ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra sagon Vc agon Win and Net MDM920 M96351 M9650, M8996 <i>A</i> D5, Qual	ing in to SUI to odragon gon gon agon agon bice & red working 06, M,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 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	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239							
N/A	25-07-2019	2.1	surface Error h checked unpred Snapdr Compu Connec Consum Industr IoT, Sna Snapdr Infrastr in IPQ4 IPQ807 MDM92 MDM92 MDM96 MSM89 QCA65 QCA65 QCA65	019, IPO 4, MDM 206, MD 640, MD 96AU, Q 64, QCA 74AU, Q 84AU, Q 77, QCA	to the s is not part is not part opehaviou to, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra Snapdra Snapdra (Snapdra Snapdra Snapdra Snapdra (Snapdra S	AA, CA9531, CA9531, Son Son CA9580, Soo5,	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)				551						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130		
			CVE ID : CVE-2019-2240		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1020
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1021
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253							
Informatio n Exposure	25-07-2019	7.5				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	_	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1023
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_4- 130819/1024
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Ра	tch	NCIIP	CID
			670, SI SD 845 SDX20 Snapdr	2, SD 712 0 820, SI 0 / SD 85 , ragon_Hi 0 : CVE-2	0 820A, 0, SDM6 gh_Med	SD 835, 560, _2016				
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2264Buffer overflow can occur indisplay function due to lack ofvalidation of header block sizeset by user. in SnapdragonAuto, Snapdragon ConsumerIOT, Snapdragon IndustrialIOT, Snapdragon IndustrialIOT, Snapdragon Nobile,Snapdragon Wearables inMDM9206, MDM9607,MDM9650, MSM8909W,MSM8996AU, SD 210/SD212/SD 205, SD 425, SD 427,SD 430, SD 435, SD 450, SD615/16/SD 415, SD 625, SD636, SD 650/52, SD 712 / SD				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272		
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1028
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1029
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630 SDM660, SDX24	,	
			CVE ID : CVE-2019-2277		
Improper Authentica tion	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425 SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660	w.codeauro ra.org/secu rity- bulletin/20	0-QUA-SD_4- 130819/1030
			CVE ID : CVE-2019-2278		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439 SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1031
CV Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2279		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1032
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1033
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description 8	Pat	ch	NCIIF	PC ID	
			MSM8909W, MSM QCS605, Qualcom 210/SD 212/SD 2 SD 427, SD 430, S 439 / SD 429, SD 4 SD 632, SD 636, S 675, SD 712 / SD SD 730, SD 820, S 835, SD 845 / SD 8 SD 8CX, SDA660, S SDM630, SDM660 Snapdragon_High SXR1130 CVE ID : CVE-201					
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition will DMA buffer in jpe Snapdragon Auto, Connectivity, Snap Consumer IOT, Sn Industrial IOT, Sn Mobile, Snapdrage in MSM8909W, M QCS605, SD 425, S 430, SD 435, SD 4 SD 636, SD 712 / S 670, SD 820, SD 8 SD 845 / SD 850, S SDM660, SDX20, S CVE ID : CVE-201	https:, w.cod ra.org rity- bulleti 19/07 july-2 code- aurora securi bulleti	eauro /secu in/20 7/01/ 019- a- ty-	0-QUA- 130819		
Improper Validation of Array Index	25-07-2019	7.2	Firmware is gettin of overwriting me scan command is host because of in validation. in Snap Compute, Snapdra Consumer IOT, Sn Industrial IOT, Sn Mobile, Snapdrago Music, Snapdrago Infrastructure and	https:, w.qua m.com mpany duct- securi ulletin	lcom 1/co y/pro ty/b	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID			ID	Pa	tch	NCIIF	PC ID
			in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346							
			CVE ID) : CVE-2	2019-23	846				
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto,				w.cod ra.org rity-	//ww leauro g/secu in/20	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290	19/07/01/ july-2019- code- aurora- security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605 SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670 SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660 SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1038
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon	https://ww w.codeauro ra.org/secu rity-	0-QUA-SD_4- 130819/1039
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 562	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 Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2293	bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1040
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019-	0-QUA-SD_4- 130819/1041
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIP	PC ID
			Industr Mobile Music, Infrast in IPQ4 IPQ807 MDM9 MDM9 MDM9 QCA65 QCA93 SD 210 425, SI SD 210 425, SI SD 450 636, SI SD 670 820A, S 850, SI SDX24	4019, IP(74, MDM 206, MD 640, MD 996AU, (74AU, Q 77, QCA 0/SD 212 0 427, SI 0, SD 600 0 675, SI 0, SD 730 SD 835, SI 0 855, SI	Snapdra ragon Vo agon Win and Net Q8064, (9150, M9607, M9650, QCA617 (CA8081 9379, Q (CA8081 9379, Q (CA8081 9379, Q (CA6017 (CA8081 9379, Q (CA8081 9379, Q (CA809, Q (CA8081 9379, Q (CA8081 9379, Q (CA809, Q (CA809, Q (CA	agon bice & red working 4A, , CS605, 5, SD D 435, 5, SD SD 710 /), SD / SD SDX20,	code- auror secur bullet	a- ity-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibi read if not in 1 Snapdr Compu Consur Industr Mobile Wearal Infrast in IPQ4 MSM89 QCA99 215, SI SD 450 636, SI SD 820 855, SI	ite, Snap ner IOT, rial IOT, , Snapdr bles, Sna ructure 4019, IP(909W, M 80, QCS 0 425, SI 0, SD 625 0 712 / S 0A, SD 84	ut-of-bo ved from FIFO in ito, Snap dragon Snapdra Snapdra Snapdragon and Net 28064, ISM8996 605, Qua 5, SD 632 5, SD 632 50 710 / 55 / SD 8	ound n SPI is odragon agon agon n Wired working 6AU, alcomm SD 429, 2, SD 2, SD 2, SD 2, SD 350, SD 0, SDX24	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIP	PC ID
Out-of- bounds Read	25-07-2019	7.5	reason frame of the fran Snapdr Consur Consur Industr Mobile Music i MDM90 MSM89 QCA65 QCA93 425, SI SD 450 665, SI SD 670 820A, SI SDM66	tto, Snap tronics napdrag Snapdr Snapdra agon Vo 0150, M9607, M9650, QCA6174 CA9377 405, QCS 0 430, SI , SD 636 0 712 / S 50 845 / 0A660, S 0, SDX24	d from idating odragon agon agon ice & 4A, 5605, SD 0 435, 5, SD 50 710 / 0, SD 7 SD 5DM630, 4	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2305 Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Dat	e CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	9 10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1045
N/A	25-07-2019) 7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/	0-QUA-SD_4- 130819/1046

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			IOT, Sm IOT, Sm Snapdn Snapdn MDM9 MDM9 MSM89 QCS60 425, SI SD 439 625, SI SD 675 670, SI SD 845 SDA66 SDM66	apdrago apdrago ragon V 150, MD 650, MS 996AU, (5, Qualc 0 427, SI 9 / SD 42 0 632, SI 0 730, SI 5 / SD 85 0, SDM4 50, SDX2	gon Cons on Indus on Mobil oice & M earables M9607, M8909V QCS405, Omm 21 O 430, SI 29, SD 45 O 636, SI 29, SD 45 O 636, SI 20, SD 71 O 820A, 50, SD 85 39, SDM 0, SDX2 2019-23	trial e, usic, s in V, 5, SD D 435, 50, SD D 665, 0 / SD SD 835, 55, 1630, 4	july-2 code- auror secur bullet	a- ity-		
Out-of- bounds Read	25-07-2019	7.5	While s from fi integer since d exceed Snapdr Consur Consur Industr Mobile Music i MDM9 MDM9 MDM9 MSM89 QCA65 QCA93 205, SI SD 712 820A, S	calibrate in cache w may c th receiv ca length ito, Snap tronics napdrag Snapdra Snapdra Snapdra Snapdra 2000, 049607, 049650, 049650, 049650, 049650, 049650, 049650, 049650, 049650, 049650, 049650, 049650, 049650, 049650, 049650, 0506500, 050650, 0506500, 0506500, 050600,0000,00	d data e, An occur ved may . in odragon agon agon oice & 4A, , 212/SD D 636, 570, SD ,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_	
CV Scoring Sco (CVSS)	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	(Descriptio	on & CVE	ID	Ра	tch	NCIIP	PC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	comma potent: to lack data bu Snapdn Consur Consur Industr Mobile Music i MDM9 QCA61 QCA93 QCS60 205, SI SD 435 625, SI SD 712 730, SI SD 845 SDM63	tronics napdrag Snapdr Snapdra ragon Vc 9607, M8996A A6574A 9379, Q 0/SD 21 0 427, SI 0, SD 600 0 665, SI 0 / SD 6	a bw due fon of odragon agon agon bice & U, U, CS405, .2/SD D 430, D 430, D 675, 570, SD SD 835, 55, 524	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
sd_427_firm	iware									
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607,				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 568	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2235		
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1050

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				569						

Weakness	Publish Date	CVSS	Descriptio	on & CVE ID)	Pa	tch	NCIIP	C ID
			SXR1130						
			CVE ID : CVE-2	2019-223	6				
Improper Input Validation	25-07-2019	2.1	Sanity checks a layout which ca Corruption or o Denial of Servio Snapdragon Au Compute, Snap Connectivity, S Consumer Elec Connectivity, S Consumer IOT, Industrial IOT, Mobile, Snapdra Infrastructure in MDM9150, M MDM9607, MD MDM9640, MD MDM9640, MD MDM9655, MS QCS404, QCS60 215, SD 210/SI SD 410/12, SD 430, SD 435, SI SD 450, SD 615 625, SD 632, SI 650/52, SD 675 710 / SD 670, S SD 820A, SD 83 850, SD 8CX, SI SDM439, SDM6 SDX20, SDX24, Snapdragon_Hi SXR1130 CVE ID : CVE-2	an lead to can lead to ce in ito, Snapd dragon napdrago tronics napdrago Snapdrag agon Voice and Netw 4DM9206 M9635M, M9650, M9650, M9954U 05, Qualco 0 212/SD 425, SD 4 0 439 / SE 5/16/SD 4 0 636, SD 5, SD 712 SD 730, SE 35, SD 845 DA660, 530, SDM6	SUI o ragon n n gon ce & d orking o, , , , , , , , , , , , , , , , , , ,	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
Improper Restriction of Operations within the	22-07-2019	2.1	Possible buffer end of iterating getting the ver- lead to informa in Snapdragon	g loop whi sion info a ation discl	while w.qualcom nfo and m.com/co disclosure. mpany/pro			0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 570	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
Bounds of a Memory Buffer			in MDM MDM90 MSM89 210/SI SD 427 439 / S 615/16 632, SI SD 712 730, SI SD 845 SDA66 SDM66	IOT, ragon ice & arables 7, V, SD D 425, 5, SD D 425, 5, SD D 675, 70, SD SD 835, 5, 5, 630,	secur					
Improper Input Validation	25-07-2019	7.5	CVE ID : CVE-2019-2243 Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descrip	tion & CVE	ID	Pa	tch	NCIIPC ID	
			SD 835, SD 8 855, SDA660 SDM630, SD	, SDM439,	·				
			CVE ID : CVE	2-2019-22	53				
Informatio n Exposure	25-07-2019	7.5	Position dete accuracy may to wrongly d information Auto, Snapdu Snapdragon Snapdragon Snapdragon Mobile, Snap Music, Snapc in MDM9150 MDM9607, M MDM9607, M MDM9607, M MDM9640, M MDM9640, M MDM9640, M MDM9655, M MDM9640, M MDM9655, M MDM9640, M MDM9640, M MDM9655, M SD820, SD 4 30, SD 4 429, SD 450, 415, SD 625, SD 430, SD 4 429, SD 450, 415, SD 625, SD 650/52, S 712 / SD 710 SD 820, SD 8 845 / SD 850 SDA660, SD SDA660, SD SDA660, SD SDA660, SD SDA660, SD SDA660, SD SDA660, SD	y be degra ecoded in Snapdra agon Com Consumer Industrial IoT, Snapd dragon Vo Iragon We), MDM920 (DM9615, 1DM9635N (DM9635N (DM9635N (DM9635N) (DM9635N (DM9635N) (SD 425, SI 35, SD 439 SD 615/10 SD 632, SI SD 632, SI SD 665, SD () / SD 670, 20A, SD 83 (), SD 855, S (1439, SDM (X20, High_Med	ded due agon pute, IOT, IOT, ragon ice & arables 6, 4, V, V, V/SD 0 427, 0 / SD 0 427, 0 / SD 0 636, 675, SD 50 730, 85, SD 50 8CX, 630, 2016,	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
Use After Free	22-07-2019	6.9	A race condit processing p can lead to a condition in Snapdragon Snapdragon	erf-event v use after f Snapdrago Compute,	which ree on Auto,	w.cod ra.org rity-	//ww leauro g/secu in/20 5/03/	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
			Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 QCS40 215, SI SD 425 435, SI SD 425 665, SI SD 625 665, SI SD 730 845 / S SDM43 SDX20, Snapdr SXR113	june-2 code- auror secur bullet	a- ity-					
N/A	22-07-2019	4.9	Unauth subsyst non sec can lea disclos Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Infrastr in IPQ8 MDM90 QCA80 215, SI SD 425 435, SI	d to info ure in Sr agon Co agon Co agon Co agon Mo agon Mo agon Wi	access fr ILOS or o system i mapdrag mpute, nnectivi nsumer dustrial obile, nice & Mi ired and Netv DM9150 M9607, M8996A 505, Qua 505, Qua 505, Qua 505, Qua 505, Qua 505, Qua	om GPU other memory on Auto, ity, IOT, IOT, usic, working , U, alcomm D 205, 0, SD SD 450,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1057
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019-	0-QUA-SD_4- 130819/1058
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & C	/E ID	Pat	tch	NCIIF	PC ID
			in MDM9607, MDM9 MSM8909W, QCS40 SD 425, SD 427, SD 4 435, SD 439 / SD 42 SD 625, SD 632, SD 6 712 / SD 710 / SD 6 820A, SD 835, SD 84 850, SDM439, SDM6 SDM660, SDX24 CVE ID : CVE-2019-	5, QCS605, 30, SD 9, SD 450, 36, SD 70, SD 5 / SD 30,	code- aurora securi bullet	ty-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2264 Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272		https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin		0-QUA-SD_4- 130819/1059	
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins		0-QUA-SD_4- 130819/1060	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273			
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1061	
Improper Authentica tion	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 /	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-	0-QUA-SD_4- 130819/1062	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 710 / SD 670, SD 845 / SD 850, SDM660 CVE ID : CVE-2019-2278	security- bulletin	
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1063
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1064
CV Scoring So (CVSS)	cale 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	Pat	tch	NCIIF	PC ID	
			SD 632, SD 636 675, SD 712 / S SD 730, SD 820 835, SD 845 / S SD 8CX, SDA66 SDM630, SDM6	Yearables in ISM8996AU, omm 215, SD D 205, SD 425, D, SD 435, SD SD 450, SD 625, 6, SD 665, SD SD 710 / SD 670, D, SD 820A, SD SD 850, SD 855, 60, SDM439, 660, igh_Med_2016,				
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	DMA buffer in Snapdragon Au Connectivity, S Consumer IOT, Industrial IOT, Mobile, Snapdu in MSM8909W QCS605, SD 42 430, SD 435, SI SD 636, SD 712	ato, Snapdragon inapdragon , Snapdragon Snapdragon ragon Wearables 7, MSM8996AU, 5, SD 427, SD D 450, SD 625, 2 / SD 710 / SD D 820A, SD 835, 50, SDA660, 20, SDX24	https: w.cod ra.org rity- bullet 19/07 july-2 code- aurora securi bullet	eauro /secu in/20 7/01/ 019- a- ty-	0-QUA- 130819	_
Improper Validation of Array Index	25-07-2019	7.2	Firmware is ge of overwriting scan command host because o validation. in S Compute, Snap Consumer IOT, Industrial IOT, Mobile, Snapdi	https: w.qua m.con mpan duct- securi ulletir	lcom 1/co y/pro ty/b	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCII	PC ID
			Music, S Infrastr in IPQ8 QCS404 425, SD SD 450, 712 / S SD 835, 855, SD SDM63 CVE ID							
Out-of- bounds Write	22-07-2019	7.5	CVE ID : CVE-2019-2346 Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Use After Free	25-07-2019	4.6	Multiple multiple camera	e thread	ls will le	ead	w.cod	//ww leauro g/secu	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	CID
			destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290					a- ity-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	CVE ID : CVE-2019-2290 Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to			-	//ww eauro	0-QUA- 130819		
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lack of length check of in por resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearable in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625 SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 84 SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2293	rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info v macro which can lead to use after-free in Snapdragon Aut Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427 SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 71 SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298	 - https://www.qualcomm.com/company/product-security/bulletins 0 / 	0-QUA-SD_4- 130819/1071
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can b triggered by a specially-craft command supplied by a userspace application. in Snapdragon Auto, Snapdrago	ed w.codeauro ra.org/secu rity-	0-QUA-SD_4- 130819/1072
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 581	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	tch	NCIIP	C ID
			Connec Consum Industr Mobile, Music, S Infrastr in IPQ4 IPQ807 MDM92 MDM92 MDM92 MDM92 MDM92 SD210 425, SE SD 450 636, SE SD 670 820A, S 850, SE SDX24	019, IP(74, MDM 206, MD 540, MD 996AU, Q 74AU, Q 77, QCA 77, QCA 75D 212 9427, SE , SD 600	napdrag Snapdra Snapdra agon Vo gon Wir and Netw 28064, 9150, M9650, 0430,51, 0430,51 050,50,50 0512/5 0512/5 050,820 50,845/ 0M660,5	agon agon ice & red working 4A, 5, SD 5, SD	19/07 july-2 code- auror securi bullet	019- a- ity-		
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD				w.cod	7/01/ 019- a- ity-	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1074
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-	O-QUA-SD_4- 130819/1075
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	PC ID
			Snapdr MDM9 MDM9 QCA61 QCA93 QCS60 205, SI SD 435 625, SI SD 712 730, SI SD 845 SDM63 SDX24	ragon M ragon Vc 150, MD 607, MD 650, MS 74A, QC 77, QCA 5, SD 21 0 425, SI 0 425, SI 0 425, SI 0 425, SI 0 425, SI 0 425, SI 0 50 450 0 636, SI 0 820, SI 0 820, SI 0 850 0, SDM6	oice & M M9206, M9640, M89964 A6574A 9379, Q 0/SD 21 0 427, S 0, SD 600 D 665, S 0 / SD 60 D 820A, 50, SD 85 560, SDX	AU, IU, CS405, 2/SD D 430, 0, SD D 675, 570, SD SD 835, 55, (20,	secur			
N/A	25-07-2019	7.2	User ap potenti the fast driver to go th subsys Auto, S IOT, Sm IOT, Sm IOT, Sm Snapdr MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MSM89 QCS60 425, SI SD 439 625, SI SD 675 670, SI SD 845 SDA66	oplicatio ially mal trpc driv will allo nrough t tem in S napdrago apdrago apdrago cagon Vo 5, Qualco 5, Qualco 5, Qualco 0 427, SI 0 427, SI 0 632, SI 5, SD 712	on could ke RPC of ver and t w the m to the re napdrag gon Cons on Indus on Mobil oice & M earables M9607, M8909V QCS405, 0M8909V QCS405, 0M8909V QCS405, 0M9607, M8909V QCS405, M8909V QCS405, M8909V QCS405, M8909V QCS405, M8909V QCS405, M8909V QCS405, M8909V QCS405, M8909V QCS405, M8909V QCS405, M8909V QCS405, M8909V QCS405, M8909V QCS405, M8909V QCS405, M8909V QCS405, M800,	call to the essage mote gon sumer strial le, usic, s in V, 5, SD D 435, 50, SD D 435, 50, SD D 665, 10 / SD SD 835, 55, 1630,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

V Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1
				584						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2308		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1077
sd_429_firm	nware				<u> </u>
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1078
CV Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	C ID
			in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2235							
NULL Pointer Dereferenc e	25-07-2019	2.1	Null po during termin applica Auto, S Snapdn					//ww ilcom n/co y/pro ity/b ns	0-QUA- 130819	_
CV Scoring So	cale 0-1	1-2	2-3	agon_Hi	gn_Med 4-5	_2016, 5-6	6-7	7-8	8-9	9-10
(CVSS)				5.96						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130		
			CVE ID : CVE-2019-2236		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239	w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1080
Improper Restriction of Operations within the	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto,	https://ww w.qualcom m.com/co mpany/pro duct-	0-QUA-SD_4- 130819/1081
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 587	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	escriptio	n & CVE	ID	Pa	tch	NCIIP	CID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243				securi	• •		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A,				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1083
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/	O-QUA-SD_4- 130819/1084
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670 SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260	, june-2019- code- aurora- security- bulletin	
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD	y https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1085
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2261		
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1086
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1087
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2273		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1088
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1089
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334							
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	CVE ID : CVE-2019-2334 Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2343		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1091
			CVE ID : CVE-2019-2287		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	0-QUA-SD_4- 130819/1092
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIF	C ID
			in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301				bullet	in		
N/A	25-07-2019	7.2	potenti the fast driver to go th subsys Auto, S IOT, Sn IOT, Sn IOT, Sn IOT, Sn Snapdr MDM9 MDM9 MDM9 MDM9 MDM9 MSM89 QCS60 425, SI SD 439 625, SI SD 675 670, SI SD 845 SDA66 SDM66	oplication ially make trpc drive will allow nrough to tem in Sin napdrago apdrago apdrago agon Vo agon Vo agon We 150, MD 650, MSN 96AU, Q 5, Qualco 0427, SD 96AU, Q 5, QUALCO 140, SD 730, SD 740, SD	te RPC c er and t w the may o the ren hapdrag on Cons on Indus on Mobil ice & Mi earables M9607, M8909V QCS405, M8909V QCS405, omm 21 0 430, SI 9, SD 45 0 636, SI / SD 71 0 820A, S 0, SD 85 39, SDM 0, SDX24	he essage note on sumer trial e, usic, in V, 5, SD 0 435, 0, SD 0 435, 0, SD 0 665, 0 / SD SD 835, 55, 630, 4	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
sd_430_firm	nware									
Improper Restriction of Operations within the Bounds of	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon				w.qua m.con	n/co y/pro	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIP	C ID
a Memory Buffer			Consur Connec Consur Industr Mobile Music, Infrastr in MDM MDM90 MSM89 QCS609 410/12 430, SE SD 450 636, SE SD 820 845 / S SDM43 Snapdr SXR113	49206, M 650, MD 996AU, Q 5, Qualco 2, SD 425 0 435, SE 0 435, SE 0 712 / S 0, SD 820 SD 850, S 89, SDM6 ragon_Hi	tronics napdrag Snapdra Snapdra sagon Vo agon Win and Netw ADM960 M9655, QCS404, 0M9655, QCS404, 0M9655, QCS404, 5, SD 42 0 439 / S 5, SD 632 SD 710 / 0A, SD 83 SD 8CX, S 530, SDM agh_Med	gon agon oice & red working 07, 5, SD 7, SD 7, SD 5D 429, 2, SD 7 SD 670, 35, SD SDA660, 4660, _2016,	ulletin	ns		
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
			QCA80		605, Qua	alcomm				

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236 Sanity checks are missing in							
Improper Input Validation	25-07-2019	2.1	layout Corrup Denial Snapdr Compu Connec Consur Industr Mobile Music, Infrastr in MDM MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52 710 / S SD 820 850, SI	which ca tion or c of Servic ragon Au te, Snap ctivity, Sa ner Elec ctivity, Sa ner IOT, rial IOT, , Snapdr Snapdra ructure a (19150, M 607, MD 640, MD 655, MSI 4, QCS60 (210/SI /12, SD () 435, SI	an lead t can lead ce in ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra agon Vo gon Win and Netw ADM920 M9635N M9650, M8996A D5, Qualo D 212/S 425, SD 0 439 / S 5/16/SD D 636, SI 5, SD 71 SD 730, S S5, SD 84 D 730, S S5, SD 84	o SUI to odragon on agon ice & red working 6, 4, .U, comm D 205, 427, SD SD 429, 415, SD SD 429, 415, SD D 2 / SD SD 820, i5 / SD 1660,	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring S	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130		
			CVE ID : CVE-2019-2239		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1097
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1098
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDX20, Snapdragon_High_Med_2016,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1099

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				599						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670 SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1100
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://ww	0-QUA-SD_4- 130819/1101
CV Scoring So	cale 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	600		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1102

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				601						

		Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263		
		CVE ID : CVE-2019-2263		
22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1103
		CVE ID : CVE-2019-2264		
25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1104
			2-07-2019 4.6 MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264 Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20	2-07-20194.6in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24bulletinCVE ID : CVE-2019-2264Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20https://ww

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

9-10

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	ID	Pa	tch	NCIIF	PC ID
Out-of- bounds Read	25-07-2019	7.8	playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273 Out of bound read can happen due to lack of NULL					//ww llcom n/co y/pro ity/b ns	0-QUA- 130819	
Out-of- bounds Read	22-07-2019	4.6		w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819				
CV Scoring So	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7
				603			

9-10

7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2277		
Improper Authentica tion	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 CVE ID : CVE-2019-2278	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1107
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1108

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				604						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1109
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1110

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				60E						

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	C ID
			SDM660, SDX20, SDX24							
			CVE ID : CVE-2019-2345							
Improper Validation of Array Index	25-07-2019	7.2	of over scan co host be validat Compu Consur Indust Mobile Music, Infrast in IPQE QCS40 425, SI SD 450 712 / S SD 835 855, SI SDM63	CA8081, D5, QCS6 D 430, S G, SD 636 SD 670 G / SD 85 DA660,	y when a from per gon agon agon oice & red working 505, SD D 435, 5, SD 5, SD 5, SD 5, SD 5, SD 5, SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439 SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2287		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1113
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605	w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security-	0-QUA-SD_4- 130819/1114
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2292		
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2293	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1115
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_4- 130819/1116
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2298		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1117
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/	O-QUA-SD_4- 130819/1118
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIF	CID
			Consur Industr Mobile Music i MDM9 MSM89 QCA65 QCA93 425, SI SD 450 665, SI SD 670 820A, S 850, SI SDM66	M9607, M9650, QCA6174 CA9377 405, QCS 0 430, SI 3, SD 636 0 712 / S 0, SD 820 SD 845 / DA660, S 0, SDX2	agon agon ice & 4A, , 5605, SD 0 435, 5, SD 5D 710 / 0, SD 7 SD 5DM630, 4	july-2 code- auror secur bullet	a- ity-			
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2305 Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20		
			CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, SD 435, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1120
			CVE ID : CVE-2019-2307 User application could	https://ww	
N/A	25-07-2019	7.2	potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607,	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1121
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308						
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1122				
sd_435_firm	sd_435_firmware								
Improper Restriction of	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the	https://ww w.qualcom m.com/co	0-QUA-SD_4- 130819/1123				
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 612	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			TA rollback protection logic. Snapdragon Auto, Snapdrago Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networki in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 42 SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 6 SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA60, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 SXR1130 CVE ID : CVE-2019-2235	on duct- security/b ulletins 9, 70, 60,	
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdrago Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networki in IPQ8074, MDM9206,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1124
			MDM9607, MDM9650,		

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236							
Improper Input Validation	25-07-2019	2.1	Sanity layout Corrup Denial Snapdr Compu Connec Consur Industr Mobile Music, Infrast in MDM9 MDM9 MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52 710 / S SD 820	checks a which ca of Servic agon Au te, Snap ctivity, Si ner Elect ctivity, Si ner IOT, rial IOT, , Snapdra ructure a 49150, M 607, MD 640, MD 655, MSI 4, QCS60 210/SI (12, SD 0 435, SI	re missi an lead t can lead t can lead t can lead to, Snap dragon napdrag tronics napdrag Snapdra Snapdra gon Win and Netv 1DM920 M9635N M9650, M8996A D5, Qualo D 212/S 425, SD 0 439 / S /16/SD D 636, SI 5, SD 712 S5, SD 84	ng in o SUI to odragon gon gon agon ice & red working 06, 4, U, comm D 205, 427, SD SD 429, 415, SD D 2 / SD SD 820,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2239		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1126
			CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1127
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pat	tch	NCIIP	CID
			MDM96 MSM89 QCS409 215, SE SD 425 435, SE SD 600 625, SE SD 675 670, SE SD 835 855, SE SDM63	0 636, SI / SD 71	5AU, comm D 205,), SD SD 450, 415, SD D 665, 10 / SD D 820A, 50, SD					
Informatio n Exposure	25-07-2019	7.5	Positio accurac to wron informa Auto, S Snapdr Snapdr Snapdr Mobile, Music, a in MDM MDM90	n detern cy may b ngly deco ation in 1 napdrag ragon Co ragon Ind ragon Io7 , Snapdra 49150, MD 625, MD 625, MD 640, MD 625, MD 640, MD 655, MSI 996AU, Q mm 215 0 205, SI 996AU, Q mm 215 0 205, SI 0 205, SI 0 450, SI 0 52, SD 50 710 / 0 850, S	nination oded Snapdra on Com nsumer dustrial F, Snapd agon Vo gon We (DM920 M9615, M9635N M9650, M96350, M9650, M96350, SD 210 O 425, SI (SD 210 O 425, SI (SD 439 O 615/10 O 632, SI 665, SD SD 670, A, SD 83 SD 855, S	agon pute, 10T, 10T, 10T, 1agon bice & arables 06, 4, 7, 9, 5D 0, 5D 0, 5D 0, 5D 0, 5D 7, 30, 50 7, 50 50 50 50 50 50 50 50 50 50 50 50 50	w.qua m.con mpan duct- securi ulletin	n/co y/pro ity/b	0-QUA- 130819	
ļ	1		SDA660, SDM439, SDM630, 2-3 3-4 4-5 5-6							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1129
			CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_4- 130819/1130
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 617	6-7 7-8	8-9 9-10

						CID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261			
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-9	
CV Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263		
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1132
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1133

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				619						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2272		
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_4- 130819/1134
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1135
CV Scoring S					

	CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
_					620						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX24		
			CVE ID : CVE-2019-2277		
Improper Authentica tion	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 CVE ID : CVE-2019-2278	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1136
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1137

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				621						

Improper Restriction of Operations within the Bounds of a Memory Buffer25-07-20192.1Concurrent ExecutionConcurrent ExecutionConcurrent ExecutionConcurrent ExecutionConcurrent Execution	CVE ID : CVE-2019-2334 Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU,	https://ww	
Improper Restriction of Operations within the Bounds of a Memory Buffer25-07-20192.1Concurrent Execution25-07-20192.1	information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://ww	
Execution	QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343	w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1138
using Shared Resource with 25-07-2019 4.4 Improper Synchroniz ation ('Race Condition')	Race condition while accessing	https://ww w.codeauro ra.org/secu rity- bulletin/20	0-QUA-SD_4- 130819/1139

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				622						

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	CID
			SDM66	50, SDX2	50, SDA6 0, SDX24					
					2019-23					
Improper Validation of Array Index	25-07-2019	7.2	of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346 Improper validation for inputs				w.qua m.cor	y/pro ity/b	0-QUA- 130819	
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD				w.cod ra.org rity- bullet 19/00	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	C ID
			SD 625 665, SI SD 670 820A, S 850, SI	, SD 730 SD 835, S	2, SD 636 D 712 / S D, SD 820 SD 845 / DA660, S	5, SD SD 710 /), SD ′ SD SDM439,				
			CVE ID : CVE-2019-2287							
Use After Free	25-07-2019	4.6	multip camera destroy in Snapdi Snapdi Snapdi Snapdi Snapdi MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 SN636 SD 636 SD 710 820A, SI S50, SI Snapdi	le open a le thread a driver f yed sess odragon Co cagon Co cagon Co cagon Mo cagon M 206, MD 640, MD	ds will le to access ion data Auto, onnective dustrial obile, earables M9607, M9650, SM8996 5, SD 42 O 450, SI 0/52, SD 20, SD 82 SD 845 / SDX20, S igh_Med	ead pointer ity, IOT, IOT, IOT, in 5AU, 7, SD 5AU, 7, SD 5625, 712 / 20, SD 'SD 5DX24, _2016	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU,				w.cod ra.org rity- bullet 19/06	a-	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Use After Free25-07-20194.6QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 430, SD 435, SD 665, SD 712 / SD 730, SD 835, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 805, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24builetinUse After Free25-07-20194.6Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Noice & Music, Snapdragon Noie & Music, Snapdragon Musie, Snapdragon Noie & Musie, Snapdragon Noie & Musie, Snapdr	Weakness	Publish Date	CVSS	Description & CV	EID	Pa	tch	NCIIF	PC ID
Use After Free25-07-20194.6freeing IFE resources due to lack of length check of in port resource. in Snapdragon (Consumer IOT, Snapdragon Industrial IOT, Snapdragon Woedshop, Spapdragon Spapdragon Woedshop, Spapdragon Woedshop, Spapdragon Woedshop, Spapdragon Woedshop, Spapdragon Woedshop, Spapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Woedshop, MDM9050, MDM9206, MDM90650, MDM9206, MDM9650, MDM90650, SD 210/SDhttps://wwhttps://ww				SD 210/SD 212/SD 2 425, SD 427, SD 430, SD 450, SD 625, SD 63 665, SD 712 / SD 710 SD 730, SD 820A, SD 8 845 / SD 850, SD 855 SDM630, SDM660, SD SDX24	D5, SD SD 435, 36, SD / SD 670, 335, SD , SDA660, X20,	bullet	in		
Use After Free25-07-20194.6accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SDhttps://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins		25-07-2019	4.6	freeing IFE resources lack of length check o resource. in Snapdrag Consumer IOT, Snapd Industrial IOT, Snapd Mobile, Snapdragon W Music, Snapdragon W in MSM8909W, QCS4 QCS605, SD 425, SD 4 430, SD 435, SD 450, S SD 636, SD 675, SD 7 710 / SD 670, SD 730 SD 850, SD 855, SDM6 SDM660, SDX24	w.cod ra.org rity- bullet 19/07 july-2 code- auror securi	eauro s/secu in/20 7/01/ 019- a- ity-	e	—	
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		25-07-2019	4.6	accessing md session macro which can lead after-free in Snapdrag Snapdragon Compute Snapdragon Consume Snapdragon Industria Snapdragon Mobile, Snapdragon Voice & M Snapdragon Wearable MDM9150, MDM9200 MDM9607, MDM9640	w.qua m.con mpan duct- securi	lcom n/co y/pro ity/b	-		
(CVSS)		cale 0-1	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2298		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1146
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20	0-QUA-SD_4- 130819/1147
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1148
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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, SDM439, SDM630, SDM660, SDX20		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	CVE ID : CVE-2019-2306 Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	0-QUA-SD_4- 130819/1149
		SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835 SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307			
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1150
CV Scoring So (CVSS)	cale 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	Descripti	on & CVE II	D	Pat	ch	NCIIP	CID
				MDM9150, MI MDM9650, MS MSM8996AU, QCS605, Qualo 425, SD 427, S SD 439 / SD 42 625, SD 632, S SD 675, SD 712 670, SD 730, S SD 845 / SD 83 SDA660, SDM4 SDM660, SDX2 CVE ID : CVE-2	M8909W QCS405, comm 215 D 430, SD 29, SD 450 D 636, SD 2 / SD 710 D 820A, S 50, SD 855 439, SDM6 20, SDX24	5, SD 435, 0, SD 665, 0 / SD D 835, 5, 530,				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-20	19	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312		https: w.cod ra.org rity- bullet 19/07 july-2 code- aurora securi bullet	eauro /secu in/20 /01/ 019- a- ty-	0-QUA- 130819	_	
sd_439_firm	iware									
Improper Restriction	25-07-20	19	4.6	Buffer overflor emulated RPM	https: w.qua		0-QUA-	SD_4-		
	cale									

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2235	m.com/co mpany/pro duct- security/b ulletins	130819/1152
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1153
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			MDM9 QCA80 215, SI 427, SI SD 429 632, SI 675, SI SD 730 835, SI SDM43 Snapdr SXR113) 410/12) 430, SI), SD 450) 636, SI) 712 / S), SD 820) 8CX, SI 89, SDM6 ragon_Hi	M8996A 605, Qua 2, SD 42 0 435, Sl 0, SD 625 0 650/5 SD 710 / 0, SD 820 0A660, 530, SDN igh_Med	AU, alcomm 5, SD D 439 / 5, SD 2, SD 2, SD 7 SD 670, 0A, SD M660, 1_2016,				
Improper Input Validation	25-07-2019	2.1	Sanity layout Corrup Denial Snapdr Compu Consur Consur Industr Mobile Music, Infrast in MDM MDM9 MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52	checks a which ca of Servio ragon Au ite, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, , Snapdra ructure A9150, M 607, MD 640, MD 655, MS 4, QCS60 0 210/SI 0/12, SD 0 435, SI	are missi an lead t can lead t can lead to, Snap dragon napdrag tronics napdrag Snapdra Snapdr	ing in to SUI to odragon gon agon agon oice & red working D6, M, AU, comm D 205, 427, SD SD 429, 0 415, SD D 2 / SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
			SD 820	A, SD 83		45 / SD				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2239		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1155
			Buffer over-read can occur while parsing an ogg file with a	https://ww	
Improper Input Validation	25-07-2019	7.5	while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1156
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 632	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	0	Descriptio	on & CVE	ID	Pat	tch	NCIIP	CID
			MDM9 MDM99 MSM89 QCS409 215, SE SD 425 435, SE SD 600 625, SE SD 675 670, SE SD 835 855, SE SDM63	ragon Wo 150, MD 607, MD 909W, M 5, QCS60 9210/SI , SD 427 9439 / S 0439 / S 0439 / S 050, SD 615 9632, SE 050, SD 712 9730, SE 0730, SE 0740, SE 0750, SE 0	M9206, M9650, SM8996 5, Qualo 212/S , SD 430 5, Qualo 212/S , SD 430 5, Qualo 212/S , SD 430 5, SD 430 636, SD 200 820, SD 200 560, SDX	5AU, comm D 205, 0, SD SD 450, 415, SD D 665, 0 / SD D 820A, 0, SD 20				
Informatio n Exposure	25-07-2019	7.5	Positio accurac to wron inform Auto, S Snapdr Snapdr Snapdr Mobile Music, in MDM MDM90 MD0 MD0 MD0 MD0 MD0 M0 MD0 M0 MD0 M0 MD0 M0 M0 M0 M0 M0 M0 M0 M0 M0 M0 M0 M0 M0	n detern cy may b ngly dece ation in napdrag ragon Co ragon Io ragon Io ragon Io ragon Io ragon Io ragon Io ragon Io ragon Io ragon So ragon Io ragon Io ragon Io ragon Io ragon So ragon Io ragon Io ragon Io ragon Io ragon Io ragon So ragon Io ragon Io rag	nination e degra oded Snapdra gon Com nsumer dustrial F, Snapd agon Vo gon We (DM920 M9615, M9635N M9650, M9650, M8909V QCS605, SD 210 O 425, SI , SD 210 O 425, SI , SD 210 O 615/10 O 632, SI 665, SD SD 670, A, SD 83	ded due agon pute, IOT, IOT, ragon ice & arables 6, 4, V, V, O/SD O 427, O / SD O 427, O / SD O 427, O / SD O 636, 675, SD SD 730, 35, SD	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1158
			CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_4- 130819/1159
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 634	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 IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261		
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1160
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in	https://ww w.qualcom m.com/co	0-QUA-SD_4- 130819/1161
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 635	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273				mpan duct- secur ulletin	• •		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5					w.cod ra.org rity- bullet 19/06	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 636	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SE 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1163
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1164
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1165

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
638										

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Ра	tch	NCIIP	C ID
			SDX24							
				: CVE-2						
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	read if not in 1 Snapdu Compu Consur Industr Mobile Wearal Infrast in IPQ4 MSM89 QCA99 215, SI SD 450 636, SI SD 820 855, SI	te, Snap ner IOT, rial IOT, , Snapdr bles, Sna ructure 019, IP(009W, M 80, QCS 0425, SI 0425, SI 0712 / S	ved from FIFO in ito, Snap dragon Snapdra Snapdra Snapdragon opdragon and Net Q8064, ISM8996 605, Qua 5, SD 632 5, SD 632 5, SD 632 5, SD 632 5, SD 632	n SPI is odragon agon n Wired working 6AU, alcomm SD 429, 2, SD 7 SD 670, 350, SD 2, SD	w.cod ra.org rity- bullet 19/0 july-2 code- auror secur bullet	a- ity-	0-QUA- 130819	
N/A	25-07-2019	7.2	potent the fast driver to go th subsys Auto, S IOT, Sm IOT, Sm IOT, Sm Snapdn Snapdn MDM9 MSM89 QCS60 425, SI SD 439 625, SI	oplicatio ially mal trpc driv will allo nrough t tem in S napdrago apdrago apdrago ragon Vc ragon W 150, MD 650, MS 996AU, (5, Qualc 0 427, SI 9 632, SI 0 632, SI	ke RPC c ver and t w the m o the rep napdrag gon Cons on Indus on Mobil bice & M earables M9607, M8909V QCS405, omm 21 O 430, SI c9, SD 45 O 636, SI	che essage mote gon sumer ctrial le, usic, s in V, 5, SD D 435, 50, SD D 665,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Ра	tch	NCIIF	PC ID
			SD 845 SDA66	0 730, SD / SD 85 0, SDM4 0, SDX2	0, SD 85 39, SDM	5, 1630,				
			CVE ID	: CVE-2	019-23	08				
sd_450_firm	iware		<u> </u>							
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	emulati sector s TA roll Snapdr Compu Connec Consum Consum Industr Mobile, Music, S Infrastr in MDM MDM96 MSM89 QCS605 410/12 430, SE SD 450 636, SE SD 820 845 / S SDM43 Snapdr SXR113 CVE ID	49206, M 650, MD 96AU, Q 5, Qualco 2, SD 425 0 435, SD 0 712 / S 0 712 / S 0 712 / S 0 850, S 0 850, S 9, SDM6 agon_Hi 30 • CVE-2	B is used imption otection ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra agon Vo gon Win and Net 1DM960 M9655, QCS404, 0M9655, QCS404, 5, SD 42 0 439 / S 5, SD 42 0 439 / S 5, SD 42 0 710 / A, SD 83 50 8CX, S 50 8CX, S	l due to s in the logic. in odragon agon agon ice & red working 07, 5, SD 7, SD 5, SD 7, SD 5D 429, 2, SD 5D 429, 2, SD 5D 670, 35, SD 5D A660, 1660, _2016, 35	w.qua m.cor mpan duct- secur ulletin	y/pro ity/b ns	0-QUA- 130819	
NULL Pointer Dereferenc e	25-07-2019	2.1	during termina applica Auto, S	SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2235 Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,				://ww alcom n/co y/pro ity/b	0-QUA- 130819	
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	<mark>3-4</mark> 640	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	PC ID
			Electro Snapdr Snapdr Snapdr Snapdr Snapdr Infrastr in IPQ8 MDM9 QCA80 215, SI 427, SI 427, SI 5D 429 632, SI 675, SI SD 730 835, SI SDM43 Snapdr SXR113	3074, MI 607, MD 655, MS 81, QCS 0 410/12 0 430, SI 0 430, SI 0 5D 450 0 636, SI 0 712 / S 0, SD 820 0 8CX, SI 39, SDM6 ragon_Hi	nnectivit onsumer dustrial obile, oice & M ired and Net DM9206 0M9650, M8996A 0M9650, QM8996A 0M9650, QM8996A 0M9650, QM9650, QM9650, SD 710 / 0, SD 820 DA660, 630, SDN igh_Med	ty, IOT, IOT, usic, working , AU, alcomm 5, SD D 439 / 5, SD 2, SD 2, SD 2, SD 2, SD 2, SD 2, SD 439 / 5, SD 439 / 5, SD 2, SD 439 / 5, SD 439 / 5, SD 2, SD 439 / 5, SD 2, SD 439 / 5, SD 2, SD 439 / 5, SD	ulletin	15		
Improper Input Validation	25-07-2019	2.1	layout Corrup Denial Snapdr Compu Connec Consur Consur Industr Mobile Music, Infrastr in MDM MDM9 MDM9	checks a which ca otion or c of Servic cagon Au ite, Snap ctivity, Si ner Elec ctivity, Si ner IOT, rial IOT, snapdra ructure a 49150, M 607, MD 640, MD	an lead t can lead ce in ito, Snap odragon napdrag ctronics napdrag , Snapdra Snapdra sagon Vo agon Win and Net MDM920 0M96350,	to SUI to odragon gon gon agon agon oice & red working D6, M,	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring Sc			4							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SI 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SI 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239)	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1171
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIP	PC ID
Improper Input Validation	25-07-2019	7.5	while p corrup Snapdr Connec Consur Industr IoT, Sn Snapdr MDM9 MDM9 MDM9 MSM89 QCS40 215, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63	ted com ragon Au ctivity, S ner IOT, rial IOT, apdrago ragon Vo ragon W 150, MD 607, MD 607, MD 607, MD 50, QCS60 0 210/SI 5, SD 427 0 439 / S	an ogg fil ment blo ito, Snap napdrag Snapdra Snapdra Snapdra in Mobil bice & Mi earables M9206, M9650, M9650, M9650, SM8996 D5, Qualo D 212/Si 7, SD 430 SJ 429, Si SJ 50, SD 30 SJ 50, SD 30	le with a ock. in odragon agon e, usic, in 5AU, comm D 205, 0, SD 5D 450, 415, SD 5D 450, 415, SD 0 665, .0 / SD 0 820A, 50, SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
Informatio n Exposure	25-07-2019	7.5	accurat to wrot inform Auto, S Snapdr Snapdr Snapdr Mobile Music, in MDM MDM9 MDM9 MDM9	n deterr cy may b ngly dec ation in napdrag ragon Co ragon Io' agon Io' Snapdra A9150, M 607, MD 625, MD 640, MD 655, MS	be degra oded Snapdra gon Com onsumer dustrial T, Snapd agon Vo agon We MDM920 M9615, M9635N M9650, M8909V	ded due Igon pute, IOT, IOT, Iragon ice & arables 06, M,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID			Ра	tch	NCIIPC ID		
			Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254							
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD		w.cod ra.org rity- bullet 19/00	a- ity-	0-QUA- 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1175	
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1176	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263		
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1177
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	0-QUA-SD_4- 130819/1178
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272	bulletin		
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1179	
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code-	O-QUA-SD_4- 130819/1180	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID			ID	Ра	tch	NCIIPC ID		
			Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277				auror secur bullet	ity-			
Improper Authentica tion	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 CVE ID : CVE-2019-2278				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636,			w.cod ra.org rity- bullet 19/00	a- ity-	0-QUA- 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_4- 130819/1183
Improper Restriction of Operations within the Bounds of	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b	0-QUA-SD_4- 130819/1184
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343	ulletins	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2345	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1185
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper	https://ww w.qualcom m.com/co mpany/pro	0-QUA-SD_4- 130819/1186
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660	duct- security/b ulletins	
Out-of- bounds Write	22-07-2019	7.5	CVE ID : CVE-2019-2346 Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1187

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				651						

Weakness	Publish Dat	e CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			SDX24 CVE ID): CVE-2	2019-22	87				
Use After Free	25-07-2019	9 4.6	multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	9 4.6	CVE ID : CVE-2019-2290 Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD				w.cod ra.org rity- bullet 19/00 june-2 code- auror secur bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292		
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2293	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1190
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_4- 130819/1191

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				653						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2298		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1192
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1193
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description &	CVE ID	Pa	tch	NCIIP	CID
			MSM8909W, MSM QCA9980, QCS605 215, SD 425, SD 43 SD 450, SD 625, SD 636, SD 712 / SD 7 SD 820A, SD 845 / 855, SDM439, SDM CVE ID : CVE-2019					
Out-of- bounds Read	25-07-2019	7.5	Out of bound access reason code is extra frame data without the frame length in Snapdragon Auto, 3 Consumer Electron Connectivity, Snap Consumer IOT, Sna Industrial IOT, Sna Mobile, Snapdrago Music in MDM9150 MDM9206, MDM9 MDM9640, MDM90 MSM8996AU, QCA QCA6574AU, QCA9 QCA6574AU, QCA9 QCA9379, QCS4055 425, SD 427, SD 43 SD 450, SD 625, SD 665, SD 675, SD 71 SD 670, SD 730, SD 820A, SD 835, SD 8 850, SD 855, SDA6 SDM660, SDX20, S3	acted from t validating Snapdragon nics dragon pdragon pdragon n Voice &), 607, 650, 6174A, 9377, QCS605, SD 0, SD 435, 636, SD 2 / SD 710 / 820, SD 645 / SD 60, SDM630, DX24	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of while handling the to out of bound rea in Snapdragon Aut Snapdragon Conne Snapdragon Consu Snapdragon Indust Snapdragon IoT, Su	w.cod ra.org rity- bullet	//ww eauro g/secu in/20 7/01/ 019-	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306	aurora- security- bulletin	
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1196
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 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		
			CVE ID : CVE-2019-2307		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_4- 130819/1197
			CVE ID : CVE-2019-2308		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_4- 130819/1198
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

sd_615_firmware			QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24		
Improper Input 25-07	2		CVE ID : CVE-2019-2312		
Input 25-02					
	07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1199

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				658						

			SDX20, SDX24	,				
			Snapdragon_H SXR1130 CVE ID : CVE-2	igh_Med_2016, 2019-2239				
Improper Restriction of Operations within the Bounds of a Memory Buffer	-07-2019	2.1	Possible buffer end of iterating getting the ver lead to informa in Snapdragon Co Snapdragon Co Snapdragon Io Mobile, Snapdra Music, Snapdra in MDM9206, I MDM9650, MS MSM8996AU, 0 210/SD 212/S SD 427, SD 430 439 / SD 429, S 615/16/SD 41 632, SD 636, S SD 712 / SD 71	r overflow at the g loop while sion info and ation disclosure. Auto, ompute, onsumer IOT, dustrial IOT, T, Snapdragon ragon Voice & agon Wearables MDM9607, M8909W, QCS605, SD D 205, SD 425, D 205, SD 425, SD 435, SD SD 450, SD 5, SD 625, SD D 665, SD 675, 10 / SD 670, SD D 820A, SD 835, 50, SD 855, 39, SDM630,	https: w.qua m.con mpany duct- securi ulletir	lcom 1/co y/pro ty/b	0-QUA- 130819	
Improper Input 25- Validation	-07-2019	7.5	Buffer over-rea while parsing a corrupted com Snapdragon Au Connectivity, S Consumer IOT Industrial IOT, IoT, Snapdragon Snapdragon W MDM9150, MD	https: w.qua m.con mpany duct- securi ulletir	lcom 1/co y/pro ty/b	0-QUA- 130819		
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 & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1202
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	CID
			Snapdı SXR11	ragon_H 30	igh_Med	_2016,				
			CVE ID) : CVE-2	2019-22	54				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
NULL Pointer Dereferenc e	25-07-2019	7.8	happen with w Snapdu Compu Consur Industr IoT, Sn Snapdu Snapdu MDM9 MDM9 MDM9 MSM89 QCS40 215, SI SD 425	CVE ID : CVE-2019-2272 Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450,			w.qua m.cor	y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	n & CVE	ID	Pa	tch	NCIIF	C ID
			SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016							
			CVE ID	: CVE-2	019-23	34				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	to out o in Snapdra Snapdra Snapdra Snapdra Snapdra Mobile, Music, S in MDM MDM96 MSM890 QCS405 215, SD SD 425, 435, SD	andling f bound dragon Co agon Co agon Co agon Ind agon Ind Snapdra 9150, M 07, MD 07, MD 07, MD 09W, M , QCS60 210/SE SD 427 439 / S 439 / S /16/SD 636, SE / SD 71 820, SE / SD 85 0, SDM4 0, SDX20	the buff read in Auto, nnectivi nsumer dustrial G, Snapd agon Vo gon We (DM920 M9650, SM8996 (5, Qualc (5,	rer leads display ty, IOT, IOT, iCe & arables 6, 6AU, comm D 205, 0, SD 5D 450, 625, SD 5D 450, 625, SD 5D 450, 625, SD 5D 835, 55, 630,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
sd_616_firmware										
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon			w.qua m.con		0-QUA- 130819		
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			Connec Consur Consur Industr Mobile Music, Infrastr in MDM MDM90 QCS404 215, SE SD 410 430, SE SD 450 625, SE 650/52 710 / S SD 820 850, SE SDM43 SDX20, Snapdr SXR113	49150, N 607, MD 640, MD 655, MS 4, QCS60 9 210/SI /12, SD 9 435, SI , SD 615 9 632, SI 2, SD 675 2, SD 675 2, SD 670, S A, SD 83 9 8CX, SI 9, SDM6 SDX24, ragon_Hi	napdrag tronics napdrag Snapdra Snapdra Snapdra and Net ADM920 M96351 M9650, M9650, M8996A D5, Quale D 212/S 425, SD 2439 / S 5/16/SD D 636, SI 5, SD 71 SD 730, S S5, SD 84 DA660, 530, SDM	gon agon agon bice & red working 06, M, U, Comm D 205, 427, SD SD 429, 415, SD D 2 / SD SD 820, 45 / SD 4660, _2016,	securi	• •		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W,			w.qua m.con	n/co y/pro ity/b	0-QUA- 130819		
CV Scoring So		1-2	2-3	3-4						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1208
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded	https://ww w.qualcom m.com/co	0-QUA-SD_6- 130819/1209
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 664	6-7 7-8	8-9 9-10

Improper Restriction of Operations utime 25-07-20194.6Information in Snapdragon information in Snapdragon Auto, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9665, MSM8909W, MSM8996AU, QCS005, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 433, SD 435, SD 439, SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 6636, SD 650/52, SD 6635, SD 635, SD 845 / SD 845 / SD 850, SD 8455, SD 8420, SD 845 / SD 850, SD 855, SD 820, SD 846 / SD 820, SD 8204, SD 835, SD 845 / SD 850, SD 855, SD 80X, SD A660, SDM439, SDM630, SD M660, SDX20, Snapdragon Inigh_Med_2016, SXR1130https://ww w.codeauro ra.org/secu rity- bulletinImproper Restriction of Operations within the Bounds of a Memory Buffer4.6Buffer overflow can occur in display function due to lack of MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9620, SD 212/SD 212/SD 205, SD 425, SD 427, SD 427, SD 210/SD0-QUA-SD 6- 130819/1210 code- aurora- scurity- bulletin	Weakness	Publish Date	CVSS	Description & CVE ID			Pa	tch	NCIIP	CID	
Improper Restriction of Operations within the Bounds of a Memory Buffer25-07-20194.6display function due to lack of validation of header block size set by user. in Snapdragon IOT, Snapdragon Industrial IOT, Snapdragon Industrial Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM896AU, SD 210/SDhttps://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin				Auto, Sr Snapdra Snapdra Snapdra Mobile, Music, S in MDM MDM96 SD 430, 429, SD 415, SD SD 650/ 712 / SI SD 820, SD 80, SD 80,	napdrag agon Co agon Io Snapdra Snapdra Snapdra (9150, M 507, MD 525, MD 555, MD 540, MD 555, MS 96AU, Q nm 215 205, SI 450, SI 450, SI 625, SI (52, SD 0 710 / SD 820 D 710 / SD 820 D 850, S 0, SDM4 0, SDX2 agon_Hi 0	gon Com insumer dustrial F, Snapd agon Vo gon We ADM920 M9615, M9635N M9635N M9650, M8909V QCS605, SD 210 O 425, SI SD 210 O 425, SI SD 439 O 615/10 O 632, SI 665, SD SD 670, O A, SD 83 SD 855, S 39, SDM 0, gh_Med	pute, IOT, IOT, iragon ice & arables 06, 4, 7, 7, 7, 7, 7, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8,	duct- securi	ity/b		
	Restriction of Operations within the Bounds of a Memory	25-07-2019	4.6	display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD			w.cod ra.org rity- bullet 19/07 july-2 code- auror securi	eauro g/secu in/20 7/01/ 019- a- ity-	-		
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	-	cale 0-1	1-2					6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 84 / SD 850, SDM660, SDX20			
			CVE ID : CVE-2019-2272			
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing ca happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdrago Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205 SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450 SD 600, SD 615/16/SD 415, S 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SI 670, SD 730, SD 820, SD 820, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins SD	0-QUA-SD_6- 130819/1211	
Improper			CVE ID : CVE-2019-2334 Improper casting of structure	e https://ww		
Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	while handling the buffer lea to out of bound read in displa in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	ds w.codeauro ay ra.org/secu rity- bulletin/20 19/07/01/ july-2019-	0-QUA-SD_6- 130819/1212	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness			Patch	NCIIPC ID	
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20	aurora- security- bulletin	
			CVE ID : CVE-2019-2306		
sd_625_firm	nware			Γ	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1213

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				667						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2235		
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 632, SD 636, SD 650/52, SD 635, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1214
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct-	0-QUA-SD_6- 130819/1215
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 668	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239	security/b ulletins	
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1216
CV Scoring Sc	cale 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	Ра	tch	NCIIP	PC ID
			Snapdr Infrast in IPQ4 IPQ807 MDM9 MDM9 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 QCA93 QCA98 QCN55 SD 210 425, SI SD 675 670, SI SD 835 855, SI SDM63 SDX24	4019, IP(74, MDM 206, MD 640, MD 996AU, (64, QCA 74AU, Q 84AU, Q 77, QCA	ired and Net 28064, 9150, M9607, M9650, 2CA6174 CA6584 CA8081 9379, Q 9886, Q 404, QC 2/SD 20 2/SD 20 2/SD 20 2/SD 20 5/SD 71 0 820, SI 5/SD 85 0A660, 560, SDX 30	working 4A, , , CA9531, CA9980, 5605, 5, SD D 636, 0 / SD D 820A, 50, SD 2 820A, 50, SD				
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	end of getting lead to in Snap Snapdr Snapdr Snapdr Snapdr Mobile Music, in MDM MDM9 MSM89 210/SI SD 427 439 / S	le buffer iterating informa odragon cagon Co cagon Co cagon Io cagon Io , Snapdra A9206, M 650, MS 996AU, C 0 212/SI 7, SD 430 50 429, S 6/SD 41	g loop wision info sion info ation dis Auto, mpute, msumer dustrial T, Snapo agon Vo agon We ADM960 M8909V QCS605, D 205, S D 205, S D 205, S	hile and closure. IOT, IOT, Iragon ice & arables 7, V, SD D 425, 5, SD SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660		
			CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM950, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1218
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1219
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 671	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
Use After Free	22-07-2019	6.9	CVE ID : CVE-2019-2254 A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1221
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto,	https://ww w.codeauro ra.org/secu rity-	0-QUA-SD_6- 130819/1222
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 673	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & C	VE ID	Pat	tch	NCIIP	C ID
			Snapdragon Connect Snapdragon Consum Snapdragon Industr Snapdragon Mobile, Snapdragon Wearab Snapdragon Wired Infrastructure and N in IPQ4019, IPQ806 MDM9206, MDM960 MDM9640, MDM960 MDM9640, MDM960 MDM9640, MDM960 MDM9640, MDM960 SD8020, SD 427, SD 430, SD 4 450, SD 625, SD 636 650/52, SD 712 / SE 670, SD 820, SD 820 SD 845 / SD 850, SD SDX20, Snapdragon_High_M	ner IOT, ial IOT, oles, letworking 4, 07, 50, 996AU, , SD 5, SD 425, 435, SD 5, SD 425, 435, SD 0 710 / SD A, SD 835, M660, led_2016	bullet 19/07 july-2 code- auror securi bullet	019- a- ity-		
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer derefer occurs for channel c while opening glink Snapdragon Auto, Su Consumer IOT, Snap Mobile, Snapdragon Music, Snapdragon Music, Snapdragon MSM8909W, QCS40 SD 425, SD 427, SD 4 435, SD 439 / SD 42 SD 625, SD 632, SD 6 712 / SD 710 / SD 6 820A, SD 835, SD 84 850, SDM439, SDM6 SDM660, SDX24 CVE ID : CVE-2019 -	ontext channel in napdragon odragon Voice & Wearables 9640, 5, QCS605, 430, SD 9, SD 450, 536, SD 70, SD 55 / SD 530,	ra.org rity-	eauro s/secu in/20 5/03/ 2019- a- ity-	0-QUA- 130819	
Improper Restriction	22-07-2019	7.5	Possible buffer over processing the high	_	//ww eauro	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 674	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pa	tch	NCIIF	CID
of Operations within the Bounds of a Memory Buffer			improp validati Snapdra Snapdra Snapdra Snapdra Snapdra MDM91 MSM89 QCS605 665, SD SD 730, 835, SD SDA660 SDX20,	agon Cor agon Cor agon Inc agon Mo agon Vo 50, MDI 96AU, Q 5, SD 625 712 / S SD 820 845 / S 0, SDM63 SDX24,	r length apdrago mpute, nsumer lustrial bbile, ice & Mu M9650, 0CS405, 5, SD 63 D 710 / , SD 820 D 850, S 30, SDM SXR113	on Auto, IOT, IOT, usic in 6, SD SD 670, 0A, SD SD 855, 660, 0	rity- bullet	a- ity-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2269 Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20		w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_		
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in				https: w.qua m.con		0-QUA- 130819	
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4 675	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE I	D	Pa	tch	NCIIP	CID
			Snapdragon Auto, Snapo Compute, Snapdragon Connectivity, Snapdrago Consumer IOT, Snapdrago Industrial IOT, Snapdrag Mobile, Snapdragon Voi Music, Snapdragon Wea in MSM8909W, QCS605 Qualcomm 215, SD 210, 212/SD 205, SD 425, SD SD 430, SD 435, SD 439 429, SD 450, SD 625, SD 650/52, SD 665, SD 675 712 / SD 710 / SD 670, SD 820, SD 845 / SD 850 855, SD 8CX, SDM439, Snapdragon_High_Med_ SXR1130	on gon gon ce & irables , /SD 427, / SD , SD SD 730, 0, SD 2016,	mpan duct- securi ulletin	• •		
Out-of- bounds Read	22-07-2019	4.6	CVE ID : CVE-2019-227 Out of bound read can h due to lack of NULL termination on user com data in WLAN in Snapdr Auto, Snapdragon Comp Snapdragon Consumer I Snapdragon Industrial I Snapdragon Mobile, Snapdragon Voice & Mu MSM8996AU, QCS405, QCS605, SD 210/SD 212 205, SD 425, SD 427, SD SD 435, SD 450, SD 625, 636, SD 665, SD 675, SD SD 710 / SD 670, SD 730 820A, SD 835, SD 845 / 850, SD 855, SDA660, SI SDM660, SDX24 CVE ID : CVE-2019-227	appen atrolled agon oute, IOT, OT, asic in 2/SD 430, SD 712 / 0, SD SD DM630, 77	w.cod ra.org rity- bullet 19/06 june-2 code- auror securi bullet	2019- a- ity- in	0-QUA- 130819	/1227
Improper Authentica	25-07-2019	7.2	User keystore signature ignored in boot and can		-	//ww eauro	0-QUA- 130819	
CV Scoring Sc (CVSS)	ale 0-1	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tion			bypass boot image signatu verification in Snapdragon Auto, Snapdragon Consum IOT, Snapdragon Mobile in MDM9607, MDM9640, SD SD 427, SD 430, SD 435, SI 450, SD 625, SD 636, SD 72 SD 710 / SD 670, SD 845 / 850, SDM660 CVE ID : CVE-2019-2278	n rity- her bulletin/20 n 19/07/01/ 425, july-2019- D code- 12 / aurora- / SD security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets upda with invalid data and may to access beyond the alloca memory. in Snapdragon A Snapdragon Connectivity, Snapdragon Consumer IO Snapdragon Industrial IO Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU QCS405, QCS605, Qualcom 215, SD 210/SD 212/SD 2 SD 425, SD 439 / SD 429, S 450, SD 625, SD 632, SD 63 SD 665, SD 675, SD 712 / S 710 / SD 670, SD 730, SD 8 SD 820A, SD 835, SD 845 / 850, SD 855, SDA660, SDM SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_20 CVE ID : CVE-2019-2279	rlead ated ated ated ated ated ated ated a	0-QUA-SD_6- 130819/1229
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing happen when playing the o with wrong block group id Snapdragon Auto, Snapdra Compute, Snapdragon	clip w.qualcom d in m.com/co	0-QUA-SD_6- 130819/1230
CV Scoring So	cale 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	Pa	tch	NCIIP	C ID
			Industr IoT, Sn Snapdr Snapdr MDM9 MDM9 QCS409 215, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63 Snapdr CVE ID) 632, SI , SD 712) 730, SI) SD 845) A660, S) A660, S (0, SDM6 ; agon_Hi) : CVE-2	Snapdra in Mobil pice & M earables M9206, M9650, SM8990 5, Qual D 212/S 7, SD 430 SD 429, S 7, SD 430 SD 429, S 6, SD 71 D 636, S 2, SD 71 D 820, S 5, SD 85 S 60, SD 85 S 80 S 80 S 80 S 80 S 80 S 80 S 80 S	agon e, usic, s in 6AU, comm D 205, 0, SD SD 450, 415, SD D 665, 10 / SD D 820A, 50, SD , (20, 2016	secur	• •		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	inform firmwa checkin structu a kerne Auto, S Snapdr SD 427	el driver napdrag ragon Co ragon Co ragon Ind ragon Wo ragon Wo 209W, M 5, Qualco 212/SI 7, SD 430 5D 429, S 5, SD 636	sclosure o insuff embedd can be se in Snap gon Com onnectiv onsumer dustrial obile, nice & M earables (SM899) omm 21 D 205, S 0, SD 435 5, SD 665	icient led ent from dragon pute, ity, · IOT, IOT, IOT, usic, s in 5AU, 5, SD D 425, 5, SD SD 625,	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 678	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptic	on & CVE	ID	Ра	tch	NCIIP	C ID
			SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130							
			CVE ID) : CVE-2	019-23	43				
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	DMA b Snapdn Connec Consur Industr Mobile in MSM QCS60 430, SI SD 636 670, SI SD 845 SDM66	uffer in j ragon Au ctivity, S ner IOT, rial IOT,	peg driv napdrag Snapdra Snapdra agon W , MSM89 5, SD 42 0 450, SI 2 / SD 71 0 820A, 5 0, SDA6 0, SDX2	odragon gon agon earables 996AU, 7, SD D 625, 10 / SD SD 835, 60, 4	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660,				w.qua m.cor mpan duct- secur ulletin	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, SDM660		
			CVE ID : CVE-2019-2346		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1234
Use After Free CV Scoring So	25-07-2019	4.6	CVE ID : CVE-2019-2287 Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1235
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290			
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670 SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1236	
			SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292			
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1237	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24			
			CVE ID : CVE-2019-2293			
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1238	
			CVE ID : CVE-2019-2298			
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1239	
CV Scoring So (CVSS)	cale 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 & CVE ID			Pa	tch	NCIIPC ID		
				MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299							
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-0	7-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_	
Out-of- bounds Read	25-0	7-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon			w.cod ra.org rity- bullet 19/02	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019-		0-QUA-SD_6- 130819/1241	
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
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305	code- aurora- security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1242

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
684										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20		
			CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1243
			CVE ID : CVE-2019-2307 User application could	https://ww	
N/A	25-07-2019	7.2	potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607,	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_6- 130819/1244
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308		
Out-of- bounds Read	25-07-2019	7.5	CVE ID : CVE 2019-2300While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20CVE ID : CVE-2019-2309	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1245
Improper Restriction of Operations within the Bounds of	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/	0-QUA-SD_6- 130819/1246
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 686	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	july-2019- code- aurora- security- bulletin	
sd_632_firm	nware				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1247

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				687						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2235		
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1248
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in	https://ww w.qualcom m.com/co mpany/pro	0-QUA-SD_6- 130819/1249
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 688	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descrip	otion & CVE	ID	Pa	tch	NCIIP	CID
			Snapdragon Compute, Sn Connectivity Consumer E Connectivity Consumer IC Industrial IC Mobile, Snap Music, Snapo Infrastructur in MDM9150 MDM9607, M MDM9640, M MDM9640, M MDM9640, M MDM9655, M QCS404, QCS 215, SD 210, SD 410/12, S 430, SD 435, SD 450, SD 60 625, SD 632, 650/52, SD 6 625, SD 632, 650/52, SD 6 710 / SD 670 SD 820A, SD 850, SD 8CX SDM439, SD SDX20, SDX20 SNAPAGON SXR1130	apdragon , Snapdrag lectronics , Snapdrag OT, Snapdrag OT, Snapdrag OT, Snapdra OT, Snapdra OT, Snapdra OT, Snapdra OT, Snapdra OT, Snapdra (SD 439 / 4 SO 425, SD SD 425, SD SD 425, SD SD 425, SD SD 439 / 4 SO 439 / 4 SO 5, SD 71 O, SD 730, 4 SD 5, SD 84 SD 636, SD SD 636, SD SD 630, SD 630, SD SD 630, SD 630, SD SD 630, SD 630, SD SD 630, SD 640, SD 6	gon agon agon oice & red working 06, M, AU, comm D 205, 427, SD SD 429, 415, SD D 2 / SD SD 820, 45 / SD M660, _2016,	duct- secur: ulletin	• •		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,			w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660		
Improper Input Validation	25-07-2019	7.5	CVE ID : CVE-2019-2243 Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1251
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due	https://ww w.qualcom	0-QUA-SD_6- 130819/1252
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			to wroi	ngly deco	oded		m.con	1/00		
			Auto, S Snapdr Snapdr Snapdr Mobile Music, in MDM MDM90 MDM9	ation in S napdrag agon Co agon Ind agon Ind agon Ind agon Ind agon Ind snapdra 49150, M 607, MD 625, MD 625, MD 625, MD 640, MD 655, MSI 996AU, Q mm 215 0 205, SI 996AU, Q mm 215 0 205, SI 0 205, SI 0 450, SI 0 450, SI 0 52, SD 0 710 / 0, SD 820 SD 70 SD 70	Snapdra on Comj nsumer dustrial 1 F, Snapd agon Voi gon Wea 1DM920 M9615, M9635M M9650, M9635M M9650, M8909W QCS605, SD 210 D 425, SI , SD 210 D 425, SI , SD 210 D 425, SI 665, SD SD 670, A, SD 833 D 855, S 39, SDM 0, gh_Med_ 019-22	pute, IOT, IOT, ragon ice & arables 6, 1, /SD 0 427, /SD 0 427, /SD 0 636, 675, SD 50 730, 55, SD 20 8CX, 630, 2016, 54	mpan duct- securi ulletir	y/pro ty/b		
Use After Free 22	-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W,				https: w.cod ra.org rity- bullet 19/06 june-2 code- auror securi bullet	eauro /secu in/20 5/03/ 2019- a- ity-	0-QUA- 130819	
	1		MDM9	030, MSI	M8909W	/,				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1254

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				692						

Weakness	Publis	sh Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
				SXR11	30						
				CVE ID	CVE ID : CVE-2019-2261						
NULL Pointer Dereferenc e	22-07	-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264					//ww eauro s/secu in/20 5/03/ 2019- a- ity- in	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07	-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale	450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439,		SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439,				7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1257
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1258
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 694	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			Snapdr Snapdr MSM89 QCS609 210/SI SD 427 439 / S SD 632 675, SI SD 730 835, SI SD 8CX SDM63 Snapdr SXR113), SD 820) 845 / S (, SDA66 (0, SDM6 ragon_Hi 30	vice & M earables (SM8996 omm 21 D 205, S D 205, S D 450, S D 450, S D 450, S D 710 / O, SD 820 SD 850, S O, SDM4 560, gh_Med	s in 5AU, 5, SD D 425, 5, SD 5D 625, 5, SD SD 670, 0A, SD 5D 855, 39, _2016,				
Out-of- bounds Write	22-07-2019	7.5	CVE ID : CVE-2019-2343 Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439,			w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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		
			CVE ID : CVE-2019-2287		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1260
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_6- 130819/1261
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2306		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1262
sd_636_firm	iware				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1263
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Dereferenc e $ \begin{array}{c c c c c c c c c c c c c c c c c c c $	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer e25-07-20192.1during secure application termination using specific 				Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
032, 30 030, 30 030/ 32, 3D	Pointer Dereferenc	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 /	w.qualcom m.com/co mpany/pro duct- security/b	0-0UA-SD 6-
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	-	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Da	te CVSS	I	Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236							
			CVE ID	36						
Improper Input Validation	25-07-201	19 2.1	layout Corrup Denial Snapdu Compu Connee Consur Industr Mobile Music, Infrast in MDM MDM9 MDM9 MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52 710 / S SD 820 850, SI SDM43 SDX20 Snapdu SXR11	tte, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, , Snapdra Snapdra Snapdra ructure 49150, N 607, MD 640, MD 640, MD 655, MS 4, QCS60 0 210/S 0/12, SD 0/12, SD 0/12	an lead t can lead t can lead de in ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra M9650, M9650, M9650, M9650, M9650, M9650, M9650, SJ, Qual D 212/S 425, SD 2 439 / S 5/16/SD D 636, S 5, SD 71 SD 730, S S 5, SD 84 D 730, S S 5, SD 84 D 6360, S S S S S S S S S S S S S S S S S S S	ao SUI to odragon gon agon agon agon agon agon agon a	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA6174A, QCA6574AU, QCA6584, QCA6584AU, QCA6584, QCA6574AU, QCA6584, QCA6574AU, QCA6584, QCA6574AU, QCA6584, QCA6574AU, QCA6584, QCA6584AU, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1266
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading	https://ww w.qualcom m.com/co mpany/pro duct-	0-QUA-SD_6- 130819/1267
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	ſ	Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2241			securi	• •			
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD			w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	_	
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 & CVE ID	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660		
			CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1269
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1270
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 702	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730 SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
Use After Free	22-07-2019	6.9	CVE ID : CVE-2019-2254 A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670	https://ww w.codeaury ra.org/secu rity- bulletin/20 19/06/03, june-2019- code- aurora- security- bulletin	o u 0 / 0-QUA-SD_6- / 130819/1271
CV Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1272
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto,	https://ww w.codeauro ra.org/secu rity-	0-QUA-SD_6- 130819/1273
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 704	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & C	/E ID	Pa	tch	NCIIP	C ID
			Snapdragon Connect Snapdragon Consum Snapdragon Industri Snapdragon Mobile, Snapdragon Wearab Snapdragon Wired Infrastructure and N in IPQ4019, IPQ8064 MDM9206, MDM960 MDM9640, MDM965 MSM8909W, MSM89 QCA9531, QCA9980, 210/SD 212/SD 205 SD 427, SD 430, SD 4 450, SD 625, SD 636, 650/52, SD 712 / SD 670, SD 820, SD 820, SD 845 / SD 850, SD SDX20, Snapdragon_High_M CVE ID : CVE-2019- 5	er IOT, al IOT, les, etworking , 7, 0, 96AU, SD , SD 425, 35, SD SD 710 / SD A, SD 835, M660, ed_2016	bullet 19/07 july-2 code- auror securi bullet	019- a- ity-		
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264		w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Restriction	22-07-2019	7.5	Possible buffer overf processing the high l	-	//ww eauro	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269	ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2269Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20CVE ID : CVE-2019-2272	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1276
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack	https://ww w.codeauro ra.org/secu	0-QUA-SD_6- 130819/1277
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 706	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	Descriptio	on & CVE	Pa	tch	NCIIP	CID	
			receive space in Snapdr Electro Snapdr Snapdr Snapdr MDM96 QCA61 QCA61 QCA93 QCS60 50 675, SD SD 730 850, SD SDM66	k on acti ad from u n Snapdu agon Co nics Cor agon Co agon Vo 607, MSI 74A, QC 77, QCA 5, SD 630 712 / S , SD 820 0 855, SI 0, SDX2 : CVE-2	user con ragon A insumer inectivit onsumer obile, oice & M M8996A M8996A A6574A 9379, Q 6, SD 66 SD 710 / 0A, SD 84 OM630, 4		a- ity-			
Out-of- bounds Read	22-07-2019	4.6	CVE ID : CVE-2019-2276 Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277				w.cod ra.org rity- bullet 19/06	a- ity-	0-QUA- 130819	
Improper Authentica tion	25-07-2019	7.2	User ke ignorec bypass	signatur	e is n lead to nature	w.cod	//ww leauro g/secu	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 707	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660	bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	
			CVE ID : CVE-2019-2278		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1280
Improper Restriction of Operations within the Bounds of a Memory	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_6- 130819/1281
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2281		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1282
Improper Restriction of Operations	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded	https://ww w.qualcom m.com/co mpany/pro	0-QUA-SD_6- 130819/1283
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID Patch NCIIPC ID
within the Bounds of a Memory Buffer			structure that can be sent from a kernel driver in Snapdragonduct-a kernel driver in Snapdragonsecurity/bAuto, Snapdragon Compute, snapdragon Connectivity,ulletinsSnapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Voice & Music,iSnapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SDi210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SDi439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SDi675, SD 712 / SD 710 / SD 670,
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD aurora- 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ 0-QUA-SD_6- 130819/1284O-QUA-SD_6- 130819/1284
Improper Validation	25-07-2019	7.2	Firmware is getting into loop of overwriting memory whenhttps://ww w.qualcom0-QUA-SD_6- 130819/1285
CV Scoring Sc (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
of Array Index			scan co host be validat Compu Consur Industr Mobile Music, Infrast in IPQ8 QCS40 425, SI SD 450 712 / S SD 835 855, SI SDM63	m.con mpan duct- secur ulletin	y/pro ity/b					
Out-of- bounds Write	22-07-2019	7.5	CVE ID : CVE-2019-2346 Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	C ID
			SDM630, SDM660, SDX20, SDX24							
			CVE ID) : CVE-2	2019-22					
Use After Free	25-07-2019	4.6	Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD					//ww leauro g/secu in/20 7/01/ 019- a- ity- in	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD				w.cod ra.org rity- bullet 19/06 june-2 code- auror secur bullet	a- ity-	0-QUA- 130819	—
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2292		
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1289
			CVE ID : CVE-2019-2293		
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1290
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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-2019-2298		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1291
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_6- 130819/1292
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				tch	NCIIP	CID
			MSM8909W QCA9980, Q 215, SD 425, SD 450, SD 6 636, SD 712 SD 820A, SD 855, SDM43	CS605, Qua SD 439 / 5 25, SD 632 / SD 710 / 845 / SD 8 9, SDM660	alcomm SD 429, 2, SD 7 SD 670, 350, SD 9, SDX24				
			CVE ID : CVI						
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305			w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper ca while handli to out of bou in Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon	ng the buff and read in on Auto, Connectiv Consumer Industrial	fer leads display ity, IOT, IOT,	w.cod ra.org rity- bullet	//ww eauro 5/secu in/20 7/01/ 019-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	PC ID
			Music, in MDM MDM9 MSM89 QCS40 215, SI SD 425 435, SI SD 615 632, SI SD 712 730, SI SD 845 SDA66 SDM66	, Snapdr Snapdra 49150, M 607, MD 909W, M 5, QCS60 9 210/SI 5, SD 427 9 439 / S 6/16/SD 9 636, SI 2 / SD 71 9 820, SI 5 / SD 85 0, SDM4 50, SDX2	ngon We MDM92(M9650, SM8996 D5, Quale D 212/S 7, SD 430 SD 429, S 415, SD D 665, SI 0 / SD 6 D 820A, 50, SD 85 39, SDM 0	auror secur bullet	ity-			
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	CVE ID : CVE-2019-2306 Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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		
			CVE ID : CVE-2019-2307		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1296
			CVE ID : CVE-2019-2308		
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1297
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIF	PC ID
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20							
			CVE ID	: CVE-2	019-23					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendorcommand there exists apotential buffer overflow dueto lack of input validation ofdata buffer received inSnapdragon Auto, SnapdragonConsumer ElectronicsConnectivity, SnapdragonConsumer IOT, SnapdragonIndustrial IOT, SnapdragonMobile, Snapdragon Voice &Music in MDM9607,MDM9640, MSM8996AU,QCA6174A, QCA6574AU,QCA6174A, QCA6574AU,QCS605, SD 210/SD 212/SD205, SD 425, SD 427, SD 430,SD 435, SD 450, SD 600, SD625, SD 636, SD 665, SD 675,SD 712 / SD 710 / SD 670, SD730, SD 820, SD 820A, SD 835,SD 845 / SD 850, SD 855,SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312		w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819			
sd_650_firm	iware									
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer				w.qua m.con	n/co y/pro	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID			Pa	tch	NCIIP	CID	
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236				ulletin	ns		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm			w.qua m.con	n/co y/pro ity/b	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239							
Informatio n Exposure	25-07-2019	7.5	CVE ID : CVE-2019-2239Position determinationaccuracy may be degraded dueto wrongly decodedinformation in SnapdragonAuto, Snapdragon Compute,Snapdragon Consumer IOT,Snapdragon Industrial IOT,Snapdragon IoT, SnapdragonMobile, Snapdragon Voice &Music, Snapdragon Wearablesin MDM9150, MDM9206,MDM9607, MDM9615,MDM9625, MDM9635M,MDM9640, MDM9650,MDM9655, MSM8909W,MSM8996AU, QCS605,Qualcomm 215, SD 210/SD212/SD 205, SD 425, SD 427,SD 430, SD 435, SD 439 / SD429, SD 450, SD 615/16/SD415, SD 625, SD 632, SD 636,SD 650/52, SD 665, SD 675, SD712 / SD 710 / SD 670, SD 730,SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX,SDA660, SDM439, SDM630,			https: w.qua m.com mpan duct- securi ulletin	n/co y/pro ity/b	0-QUA- 130819	_	
CV Scoring Sca	le 0-1	1-2	2-3	0, SDX2	<i>.</i> 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		
			CVE ID : CVE-2019-2254		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	, , https://ww	0-QUA-SD_6- 130819/1302
			CVE ID : CVE-2019-2261 Access to freed memory can	https://ww	
Use After Free	25-07-2019	4.6	happen while reading from diag driver due to use after free issue in Snapdragon Auto Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	w.codeauro ra.org/secu	0-QUA-SD_6- 130819/1303
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIF	PC ID
			Snapdr Infrastr in IPQ4 MDM92 MDM92 MDM92 QCA952 210/SE SD 427 450, SE 650/52 670, SE SD 845 SDX20, Snapdr	:019, IP(206, MD 640, MD 099W, M 31, QCA 0 212/SI , SD 430 0 625, SE 2, SD 712 0 820, SE / SD 85	ired and Netv 28064, M9607, M9650, SM8996 9980, SI 0 205, SI 0 205	working 5AU, D 425, 5, SD D 10 / SD SD 835, 560, _2016	auror securi bullet	ity-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	display validati set by u Auto, S IOT, Sn IOT, Sn Snapdr Snapdr Snapdr MDM92 MDM92 MDM96 MSM89 212/SE SD 430 615/16 636, SE 710 / S / SD 85	overflow function ion of he iser. in S apdrago apdrago apdrago agon Vo agon Vo 206, MD 650, MSI 996AU, S 0 205, SI 0 205, SI 50 50/52 50 670, S 50, SD 415 50 670, S 50, SD 40 50, SD 40 5	n due to eader blo Snapdrag on Cons on Indus on IoT, obile, ice & Mu earables M9607, M8909V SD 210/S D 210/S	lack of ock size gon sumer trial usic, s in V, SD D 427, D 427, D 427, D 5, SD 5, SD 2 / SD , SD 845 X20	w.cod	7/01/ 019- a- ity-	0-QUA- 130819	_
Out-of- bounds Read	25-07-2019	7.8	IOMMU playing	J page fa	ult whil ideo file	e leads to	https: w.qua m.con		0-QUA- 130819	_
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4 722	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130	mpany/pro duct- security/b ulletins	
Use After Free	25-07-2019	4.6	CVE ID : CVE-2019-2273 Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1306
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd_652_firm	nware				
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1307
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1308
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIF	CID
			Mobile Music, Infrast in MDM MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52 710 / S SD 820 850, SI SDM43 SDX20 Snapdr SXR113	49150, N 607, MD 640, MD 655, MS 4, QCS60 0 210/SI 0/12, SD 0 435, SI 0, SD 615 0 632, SI 2, SD 675 SD 670, S 0 670, S 0 670, S 0 8CX, SI 89, SDM6 , SDX24, ragon_Hi	ragon Vo agon Win and Netv 4DM920 M9635N M9650, M8996A D5, Quald D 212/S 425, SD 2 439 / S 5/16/SD D 636, SI 5, SD 71 SD 730, S S 5, SD 84 DA660, 530, SDM agh_Med	vice & red working)6, M, U, comm D 205, 427, SD SD 429, 415, SD 2 / SD SD 820, 45 / SD 1660, _2016,				
Informatio n Exposure	25-07-2019	7.5	accuration of the second secon	n detern cy may b ngly dec ation in napdrag agon Co agon Ind agon Ind agon Io Snapdra 49150, M 607, MD 625, MD 625, MD 640, MD 655, MS 996AU, Q mm 215 D 205, SI	be degra oded Snapdra gon Com onsumer dustrial T, Snapd agon Vo gon We ADM920 M9615, M9635N M9650, M8909V QCS605, SD 210	ded due agon pute, IOT, IOT, lragon ice & arables 06, M, V,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	—
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2254		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1310
CV Scoring So					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				726						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1311
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1312
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20		
			CVE ID : CVE-2019-2272		
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_6- 130819/1313
			CVE ID : CVE-2019-2273		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_6- 130819/1314
CV Scoring S (CVSS)	cale 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	Pa	tch	NCIIF	PC ID
			QCS60 430, SI SD 636 SD 710 820A, S 850, SI Snapdr	909W, M 5, SD 42 0 435, SI 5, SD 650 0 / SD 67 SD 835, S 0M660, S ragon_Hi	5, SD 42 0 450, SI 1/52, SD 0, SD 82 SD 845 / SDX20, S gh_Med	7, SD 0 625, 712 / 0, SD SD DX24, _2016				
sda660_firm	nuaro		CVE ID) : CVE-2	019-22	90				
				overflov						
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	sector TA roll Snapdu Compu Connec Consur Industr Mobile Music, Infrast in MDM MSM89 QCS60 410/12 430, SI SD 450 636, SI SD 820 845 / S SDM43 Snapdu SXR112	M9206, M 650, MD 996AU, (5, Qualco 2, SD 425 0 435, SI 0, SD 625 0, SD 625 0, SD 820 5D 850, S 89, SDM6 ragon_Hi	imption otection ito, Snap dragon napdrag tronics napdrag Snapdra snapdra agon Vo gon Win and Net 4DM960 M9655, QCS404, omm 21 5, SD 42 D 439 / S 5, SD 42 D 439 / S 5, SD 632 SD 710 / A, SD 83 SD 8CX, S 530, SDN gh_Med	s in the logic. in odragon on agon ice & red working 7, 5, SD 7, SD 5D 429, 2, SD SD 429, 2, SD SD 670, 35, SD SD 670, 4660, 2016,	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
NULL	25-07-2019	2.1	· ·	ointer de			-	//ww	0-QUA-	SDA6-
Pointer CV Scoring So (CVSS)	cale 0-1	1-2	2-3	secure a	4-5	on 5-6	w.qua	7-8	8-9	9-10

Dereferenctermination using specificm.com/co130819eapplication ids. in Snapdragonmpany/product-Auto, Snapdragon Compute,Snapdragon Connectivity,security/bSnapdragon ConsumerulletinsElectronics Connectivity,Snapdragon Consumer IOT,Snapdragon Industrial IOT,Snapdragon Mobile,Snapdragon WiredInfrastructure and Networkingin IPQ8074, MDM9206,MDM9655, MSM8996AU,QCA8081, QCS605, Qualcomm215, SD 410/12, SD 425, SD	9/1316
213, 3D 410/12, 3D 423, 3D 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236	
Improper Input25-07-2019A 	
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	[Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
			MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52 710 / S SD 820 850, SI SDM43 SDX20	607, MD 640, MD 655, MS 4, QCS60 0 210/SI 0/12, SD 0/12,	D 439 / 5 5/16/SD D 636, SI 5, SD 71 SD 730, 5 35, SD 84 DA660, 530, SDM	M, U, comm D 205, 427, SD SD 429, 415, SD 2 / SD SD 820, 45 / SD 4660,				
N/A	25-07-2019	2.1	While s surface Error h checke unpred Snapdr Conned Consur Conned Consur Industr Industr IoT, Sn Snapdr Snapdr Snapdr Infrast in IPQ4 IPQ807 MDM9 MDM9	sending conten andling d results lictable l cagon Au te, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, apdrago cagon Vo cagon W ructure 4019, IP0 74, MDM 206, MD	behavior ato, Snap dragon napdrag tronics napdrag Snapdra Snapdra on Mobil oice & M ired and Net Q8064, 19150, M9607, M9650, QCA6174	lered screen, roperly ur in odragon gon agon agon e, usic, working	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	CVEID: CVE-2019-2240While rendering the layoutbackground, Error statuscheck is not caught properlyand also incorrect statushandling is being done leadingto unintended SUI behaviourin Snapdragon Auto,Snapdragon Compute,Snapdragon Connectivity,Snapdragon ConsumerElectronics Connectivity,Snapdragon Consumer IOT,Snapdragon Consumer IOT,Snapdragon Mobile,Snapdragon Mobile,Snapdragon Mobile,Snapdragon WiredInfrastructure and Networkingin MDM9150, MDM9206,MDM9607, MDM9650,MDM9655, MSM8996AU,QCS404, QCS605, SD 210/SD212/SD 205, SD 410/12, SD636, SD 675, SD 712 / SD 710 /SD 670, SD 730, SD 820, SD820A, SD 835, SD 845 / SD850, SD 855, SD 8CX, SDA660,SDM630, SDM660, SDX24,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDA6- 130819/1319

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				732						

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	CID
			SXR1130							
			CVE ID	2019-22	41					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU,				w.qua m.com	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDX20, Snapdragon_High_Med_2016,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDA6- 130819/1322

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				734						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130		
			CVE ID : CVE-2019-2254		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDA6- 130819/1323
			CVE ID : CVE-2019-2261	1	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora-	0-QUA-SDA6- 130819/1324
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269	security- bulletin	
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDA6- 130819/1325
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDA6- 130819/1326
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2281	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDA6- 130819/1327
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDA6- 130819/1328
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIP	CID
			MDM9 MDM9 MSM89 QCS40 215, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63 Snapdr	ragon Wa 150, MD 607, MD 909W, M 5, QCS60 0 210/SI 5, SD 427 0 439 / S 0 439 / S 0 632, SI 5, SD 712 0 730, SI 5, SD 845 0 A660, S 30, SDM6 ragon_Hi 0 : CVE-2	M9206, M9650, SM8996 D5, Qualo D 212/S SD 429, S (16/SD D 636, SI C 429, S (16/SD D 636, SI S 20, SI S 20, SI S 20, SD S 20, SDX gh_Med	5AU, comm D 205,), SD SD 450, 415, SD D 665, 0 / SD D 820A, 50, SD 20, SD				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of linform firmwa checkin structu a kerne Auto, S Snapdr Snap	bound re ation dis are due t ing of an ure that c el driver napdrag ragon Co ragon Co ragon Co ragon Mo ragon Wo 209W, M 5, Qualco 212/SI 7, SD 430 50 429, S 2, SD 636	ead and sclosure o insuffi embedd can be se in Snap gon Com nnectivi dustrial obile, ice & Mi earables SM8996 omm 21 D 205, S SD 435 SD 450, S D 450, S D 710 / SD 820 SD 850, S 0, SDM4	in cient ed ent from dragon pute, ity, IOT, IOT, IOT, usic, sin 5AU, 5, SD D 425, 5, SD D 425, 5, SD SD 625, 5, SD SD 670, 0A, SD SD 855,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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		
			CVE ID : CVE-2019-2343		
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2345	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SDA6- 130819/1330
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDA6- 130819/1331
Out-of-	22-07-2019	7.5	Improper validation for inputs	https://ww	0-QUA-SDA6-
CV Scoring So (CVSS)	cale 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	scription	& CVE	ID	Pa	tch	NCIIP	C ID
bounds Write			received lead to a issue in v Snapdrag Compute Consume Industria Mobile, S Music, Sr in MDM960 MDM960 MDM960 MDM960 MDM960 MDM960 SD 425, S 435, SD 4 SD 625, S 665, SD 6 SD 670, S 820A, SD 850, SD 8 SDM630 SDX24 CVE ID :	n out of video dr gon Aute e, Snapd er IOT, S al IOT, S Snapdrag 0150, MI 07, MDM 06AU, QC 02S605 210/SD 6AU, QC 6AU, QC 02S605 210/SD 5D 427, 439 / SE 5D 632, 675, SD 635, SI 855, SDA , SDM66	bound iver. in o, Snap ragon Snapdra gon Vo on Wea DM920 19640, 8909W CA6574 5, Qualc 212/SI SD 430 0 429, S SD 636 712 / S SD 820 0 845 / A660, S 50, SDX	write dragon agon ice & arables 6, V, AAU, comm D 205, 9, SD SD 450, 5, SD SD 710 / 9, SD SD 710 / 9, SD SD 30 SD 439, 20,	ra.org rity-	2019- a- ity-	130819	/1332
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bo due to bu checking from WL Snapdra Consume Industria Mobile, S Music in MDM965 QCA6574 SD 210/3 425, SD 450	uffer cop size of AN firm gon Aut er IOT, S al IOT, S Snapdra MDM91 50, MSM 4AU, QC SD 212/ 427, SD	by with input r ware in o, Snap Snapdra napdra gon Vo 150, (8996A S405, C (SD 205 430, SI	out eceived n dragon agon igon ice & U, QCS605, 5, SD 0 435,	w.cod ra.org rity-	2019- a- ity-	0-QUA- 130819	
			SD 430, 3 665, SD 2 SD 730, 9		0710/	SD 670,				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2292		
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SDA6- 130819/1334
			CVE ID : CVE-2019-2305		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SDA6- 130819/1335
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDA6- 130819/1336
sdm439_fir	mware				
Improper Restriction	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to	https://ww w.qualcom	0-QUA-SDM4-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 742	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pa	tch	NCIIP	CID
of Operations within the Bounds of a Memory Buffer			TA rolli Snapdra Comput Connec Consum Industr Mobile, Music, S Infrastr in MDM MDM96 MSM89 QCS605 410/12 430, SD SD 450, 636, SD SD 820, 845 / S SDM43 Snapdra SXR113	back pro agon Au te, Snap- tivity, Si- ner Elect tivity, Si- ner IOT, ial IOT, Snapdra cucture a 19206, M 550, MD 96AU, Q 5, Qualco 2, SD 425 9435, SE 9435, SE 9712 / S 50 820 D 850, S 9, SD 86 9, SD 80 1850, S 9, SD 80 180	napdrag tronics napdrag Snapdra Snapdra agon Vo gon Wir and Netw 4DM960 M9655, QCS404, 0 M9655, QCS404, 5, SD 427 5, SD 427 5, SD 427 5, SD 632 50 710 / A, SD 83 50 8CX, S 530, SDM gh_Med	logic. in dragon on agon ice & red working 7, 5, SD 7, SD 5D 429, 5, SD 5D 429, 5, SD 5D 670, 85, SD 5D 670, 60, 2016,	m.com mpan duct- secur: ulletin	y/pro ity/b	130819	/1337
NULL Pointer Dereferenc e	25-07-2019	2.1	CVE ID : CVE-2019-2235 Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206,			w.qua m.con	n/co y/pro ity/b	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Improper InputZ5-07-2019Z.1MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130Method SC VEV ED: CVE-2019-2236ValidationZ.1Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Consumer IDT, Snapdragon Mobile, Snapdragon Consumer Electronics Consumer Electronics Consumer Electronics Consumer Electronics Consumer Electronics Consumer Electronics Consumer 10T, Snapdragon Mobile, Snapdragon Wined MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 430, SD 435, SD 439 / SD 429, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 440, YB A45, SD 439 / SD 429, SD 440, YB A55, SD 636, SD 650/52, SD 632, SD 636, SD 650/52, SD 636, SD 636, SD 650/52, SD 636, SD 636, SD 636, SD 650/52, SD 636, SD 636, SD 650/52, SD 636, SD 636, SD 650/52, SD 632, SD 636, SD 636, SD 650/52, SD 636, SD 636, SD 636, SD 630, SD 8200,	Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Ра	tch	NCIIP	PC ID
Improper Input Validation25-07-20192.1Iayout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & MDM9607, MDM9206, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 5D 820A, SD 835, SD 845 / SD0-QUA-SDM4- 130819/1339				MDM9 QCA80 215, SI 427, SI SD 429 632, SI 675, SI SD 730 835, SI SDM43 Snapdr SXR11	655, MS 81, QCS 0 410/12 0 430, SI 0, SD 450 0 636, SI 0 712 / S 0, SD 820 0 8CX, SI 89, SDM6 ragon_Hi 30	M8996A 605, Qua 2, SD 42 0 435, SI 0, SD 625 0 650/5 50 710 / 0, SD 820 0A660, 530, SDN 1gh_Med	AU, alcomm 5, SD D 439 / 5, SD 2, SD 2, SD 7 SD 670, 0A, SD 4660, _2016,				
CV Scoring Scale	Input	25-07-2019	2.1	layout Corrup Denial Snapdn Compu Connec Consur Industr Mobile Music, Infrast in MDM MDM9 MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52 710 / S	which ca of Servie ragon Au re, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, , Snapdra ructure A9150, M 607, MD 640, MD 640, MD 655, MS 4, QCS60 0 210/SI 0/12, SD 0 435, SI 0, SD 615 0 632, SI 2, SD 679, S	an lead t can lead ce in ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra Snapdra agon Vo agon Win and Net M96351 M9650, M96355, M9650, M8996A D5, Qualo D 212/S 425, SD D 212/S 5/16/SD D 636, SI 5, SD 71 SD 730, S	to SUI to odragon gon gon agon agon agon agon agon de ced working 06, M, U, comm D 205, 427, SD SD 429, 415, SD D 2 / SD SD 820,	w.qua m.cor mpan duct- secur	alcom n/co y/pro ity/b	-	
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	-	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2239		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDM4- 130819/1340
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SDM4- 130819/1341
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 745	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pat	tch	NCIIP	CID
			MDM99 MSM89 QCS401 215, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63	MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253 Position determination						
Informatio n Exposure	25-07-2019	7.5	CVE ID : CVE-2019-2253			https: w.qua m.con mpan duct- securi ulletin	n/co y/pro ity/b	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDM4- 130819/1343
			CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SDM4- 130819/1344
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261		
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SDM4- 130819/1345
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in	https://ww w.qualcom m.com/co	O-QUA-SDM4- 130819/1346
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 748	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
			Compu Connec Consur Industr Mobile Music, in MSM Qualco 212/SI SD 430 429, SI 650/52 712 / S SD 820 855, SI Snapdr), SD 845 D 8CX, SI ragon_Hi	dragon napdrag Snapdra agon Vo gon We , QCS609 , SD 210 D 425, S1 D 425, S1 D 425, S1 S, SD 439 D 625, S1 S, SD 670, SD 670, S / SD 85 DM439,	gon agon agon bice & arables 5, 0/SD 0 427, 0 / SD 0 427, 0 / SD 5, SD 5, SD 5, SD 5, SD 5, SD 5, SD	mpan duct- secur ulletin			
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	SXR1130 CVE ID : CVE-2019-2273 Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDM4- 130819/1348
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDM4- 130819/1349
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDM4- 130819/1350

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				751						

Weakness	Publish Date	CVSS	6	Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID			
			SDX24										
			_	: CVE-2		-							
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301 Improper casting of structure while handling the buffer leads				not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301			w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819				
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10			

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIP	NCIIPC ID	
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20								
			CVE ID	: CVE-2	019-23						
N/A	25-07-2019	7.2	CVE ID : CVE-2019-2306 User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
sdm630_fir	mware								<u> </u>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	emulato sector s TA rolll Snapdr Compu Connec Consun	Imption otection Ito, Snar dragon napdrag	l due to s in the logic. in odragon gon	w.qua m.cor	y/pro ity/b	0-QUA- 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID				Patch		NCIIP	PC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130							
NULL Pointer Dereferenc e	25-07-2019	2.1	CVE ID : CVE-2019-2235 Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD				w.qua m.cor mpan duct- secur ulletin	n/co y/pro ity/b ns	0-QUA- 130819	/1355
CV Scoring So (CVSS)	cale 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 & CVE ID		Pa	tch	NCIIPC ID			
				675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130							
				CVE ID	: CVE-2	2019-22					
Improper Input Validation	25-07-203	19 2	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016,					//ww lcom n/co y/pro ty/b ns	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	L	1-2	2-3	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	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6174A, QCA6584AU, QCA6584, QCA6584AU, QCA6574, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, <tr< td=""><td>https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins</td><td colspan="2">0-QUA-SDM6- 130819/1357</td></tr<>	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDM6- 130819/1357	
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading	https://ww w.qualcom m.com/co mpany/pro duct-	0-QUA-SDM6- 130819/1358	
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			in Snap Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Infrast in MDM MDM9 QCS40 212/SI 636, SI SD 670 820A, S 850, SI SDM63 SXR113	odragon ragon Co ragon Co ragon Co ragon Co ragon Co ragon Mo ragon W ructure (19150, N 607, MD 655, MS 4, QCS6(0 205, SI 0 675, SI 0 675, SI 0 675, SI 0 675, SI 0 835, SI 60, SDM6 30	ompute, onnectivit onsumer dustrial obile, ired and Net MDM920 0M9650, M8996A 05, SD 22 D 410/1	ity, y, IOT, IOT, IOT, Working 06, U, 2, SD 2, SD 5D 710 / 0, SD 2 SD 2A660, 24,	securi			
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	end of getting lead to in Snap Snapdr Snapdr Snapdr Mobile Music, in MDM MDM9 MSM89 210/SI SD 427 439 / S	iterating informa odragon ragon Co ragon Co ragon In ragon Io , Snapdr Snapdra A9206, N 650, MS 996AU, (0 212/SI 7, SD 430 50 429, S	g loop w sion info ation dis Auto,	o and closure. IOT, IOT, lragon ice & arables 07, V, SD D 425, 5, SD SD	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
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	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660		
			CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDM6- 130819/1360
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDM6- 130819/1361
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 758	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC	D
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, S 712 / SD 710 / SD 670, SD 73 SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130	D 0,		
Use After Free	22-07-2019	6.9	CVE ID : CVE-2019-2254 A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450 SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 67), https://w w.codeau ra.org/sec rity- bulletin/2 19/06/03 june-2019 code- aurora- security- bulletin	ro cu 20 3/ 0-QUA-S 130819/	
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7	-8 8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDM6- 130819/1363
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon	https://ww w.codeauro ra.org/secu rity-	0-QUA-SDM6- 130819/1364
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 760	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24	bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	CVE ID : CVE-2019-2264 Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1365
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code-	0-QUA-SDM6- 130819/1366
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 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 Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276	aurora- security- bulletin	
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1367
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora-	O-QUA-SDM6- 130819/1368
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279	security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2281	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SDM6- 130819/1369
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SDM6- 130819/1370
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			Snapdr Snapdr MDM9 MDM9 QCS40 215, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63 Snapdr	apdrago agon Vo agon Wo 150, MD 607, MD 099W, M 5, QCS60 0 210/SI , SD 427 0 439 / S 0 439 / S 0 439 / S 0 439 / S 0 50 615 0 632, SI 0 730, SI 0 632, SI 0 730, SI 0 720, SI 0	vice & M earables M9206, M9650, SM8996 5, Quale 2, SD 429, S 5/16/SD 2, SD 429, S 5/16/SD 2, SD 71 2, SD 71 2, SD 71 5, SD 85 5,	usic, 5 in 5AU, comm D 205, 0, SD 5D 450, 415, SD D 665, 0 / SD D 820A, 50, SD 50, SD 50, SD 50, SD 50, SD				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of l inform firmwa checkin structu a kerne Auto, S Snapdr SD 427 439 / S SD 632 675, SI SD 730	bound re ation dis are due t ng of an ere that of el driver napdrag ragon Co ragon Co ragon Co ragon Mo ragon Mo ragon Wo 209W, M 5, Qualco 0 212/SI 7, SD 430 50 429, S , SD 636	ead and sclosure o insuffi embedd can be se in Snap gon Com onnectiv onsumer dustrial obile, ice & M earables SM8996 omm 21 D 205, S 0, SD 435 SD 450, S 5, SD 665 SD 710 / 0, SD 820	in icient ed ent from dragon pute, ity, IOT, IOT, IOT, USIC, SD 5, SD D 425, 5, SD SD 625, 5, SD SD 625, 5, SD SD 670, DA, SD	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2343		
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SDM6- 130819/1372
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SDM6- 130819/1373
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			215, SD 210/SD 212/SD 205 SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 45 SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 71 SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM4 SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287	50, 0 /	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occ due to buffer copy without checking size of input receiv from WLAN firmware in Snapdragon Auto, Snapdrago Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS6 SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435 SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 6 SD 730, SD 820A, SD 835, SI 845 / SD 850, SD 855, SDA6 SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	ved https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1374
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in po- resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearabl in MSM8909W, QCS405,	rt ra.org/secu rity- bulletin/20 19/07/01/ july-2019-	0-QUA-SDM6- 130819/1375
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24	security- bulletin	
			CVE ID : CVE-2019-2293		
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1376
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-	0-QUA-SDM6- 130819/1377
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20	security- bulletin	
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	CVE ID : CVE-2019-2306 Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1378

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				768						

Г

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Ра	tch	NCIIF	CID
			SDX24 CVE ID): CVE-2	2019-23	07				
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
			When	nandling	g the ven	ıdor				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2308 When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312		
sdm660_fir	mware				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2235	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDM6- 130819/1381

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				770						

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	Pa	tch	NCIIF	PC ID	
NULL Pointer Dereferenc e	25-07-2019	2.1	applica Auto, S Snapdn Snapdn Electro Snapdn Snapdn Snapdn Snapdn Infrast in IPQ& MDM9 QCA80 215, SI 427, SI SD 429 632, SI 675, SI SD 730 835, SI SDM43 Snapdn SXR113	termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 635, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236 Sanity checks are missing in layout which can lead to SUI				://ww alcom n/co y/pro ity/b ns	0-QUA- 130819	
Improper Input Validation	25-07-2019	2.1	layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &			w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819		
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIF	PC ID
			Music, Infrast in MDM MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52 710 / S SD 820 850, SI SDM43 SDX20 Snapdn SXR11 CVE ID							
N/A	25-07-2019	2.1	While s surface Error h checke unprec Snapdh Compu Connec Consur Industr Industr IoT, Sn Snapdh Snapdh Infrast in IPQ4 MDM9	sending conten andling d result: dictable ragon Au ragon Au re, Snap ctivity, S mer Elec ctivity, S mer IOT, rial IOT, ragon Vo ragon W ructure 4019, IPO 74, MDM 206, MD	the rend to the s is not p s in an behavior ito, Snap odragon napdrag ctronics napdrag ctronics napdrag ctronics napdrag on Mobil bice & M ired and Net Q8064,	lered screen, roperly ur in odragon gon gon agon e, usic, working	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 772	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptic	on & CVE	ID	Ра	tch	NCIIP	CID
			MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240							
			While	renderin	ig the lag	yout				
Improper Input Validation	25-07-2019	2.1	check i and als handlin to unin in Snap Snapdn Snap	49150, N 607, MD 655, MS 4, QCS60 205, SI	ught pro rect statu ng done SUI beha Auto, ompute, onnectivi onsumer dustrial obile, ired and Net MDM920 M8996A 05, SD 21 0 410/1 0 712 / S 0 845 /	pperly is leading aviour ity, Ly, IOT, IOT, IOT, ior, ior, SD 710 / 0, SD Y SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, SDM660, SDX24, SXR1130		
			CVE ID : CVE-2019-2241		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDM6- 130819/1386
			CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SDM6- 130819/1387
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDX20, Snapdragon_High_Med_2016,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDM6- 130819/1388
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1389
			CVE ID : CVE-2019-2260 Unauthorized access from GPU		
N/A	22-07-2019	4.9	subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SDM6- 130819/1390
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1391

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				777						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016		
			CVE ID : CVE-2019-2263		
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1392
Improper Restriction of Operations within the Bounds of a Memory Buffer Improper	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269 Buffer overflow can occur in	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin https://ww	0-QUA-SDM6- 130819/1393 0-QUA-SDM6-
		4.6	Buffer overflow can occur in	https://ww	0-QUA-SDM6-
CV Scoring So (CVSS)	cale 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	n & CVE	ID	Pa	tch	NCIIP	C ID
Restriction of Operations within the Bounds of a Memory Buffer			display validati set by u Auto, Si IOT, Sn IOT, Sn Snapdr Snapdr Snapdr MDM92 MDM96 MSM89 212/SE SD 430 615/16 636, SD 710 / S / SD 85 CVE ID	ra.org rity- bullet	a- ity-	130819	/1394			
Out-of- bounds Read	25-07-2019	10	occurs beacon of check receive space in Snapdr Electro Snapdr Snapdr Snapdr MDM96 QCA61 QCA93 QCA62 675, SD SD 730 850, SD SDM66	, SD 820. 855, SD 0, SDX24	ocessing est due on fram iser con ragon Au nsumer nectivit nsumer bile, ice & Mu 48996A A6574A 9379, Q0 5, SD 66 D 710 / A, SD 84 M630, 4	g to lack les trolled uto, y, IOT, usic in U, U, CS405, 5, SD SD 670, 45 / SD	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Out-of-	22-07-2019	4.6	CVE ID : CVE-2019-2276Out of bound read can happen			happen	https:	//ww	0-QUA-	SDM6-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 779	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pa	tch	NCIIP	C ID
bounds Read			termin data in Auto, S Snapdn Snapdn Snapdn MSM89 QCS60 205, SI SD 435 636, SI SD 710 820A, S 850, SI SDM66	lack of N ation on WLAN in napdrag agon Con agon Ind agon Vo 96AU, Q 96AU, Q 96AU, Q 96AU, Q 96AU, Q 96AJ, Q 9665, SD 0665, SD 0665, SD 0665, SD 065, SD 065, SD 065, SD 00, SDX24 0: CVE-2	user co n Snapd on Com nsumer lustrial obile, ice & Mu (CS405, 0/SD 21 0 427, SI 0 427, SI 0 427, SI 0 675, SI 0, SD 73 50 845 / 0A660, S 4	ragon pute, IOT, IOT, usic in 2/SD 0 430, 5, SD 0 712 / 60, SD ' SD 5DM630,	ra.org rity- bullet	a- ity-	130819	/1396
Improper Authentica tion	25-07-2019	7.2	CVE ID : CVE-2019-2277 User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 CVE ID : CVE-2019-2278				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	CVE ID: CVE-2019-2278 Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in				w.cod ra.org rity- bullet	a-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIF	PC ID
			SD 820 850, SI SDM63 SDX24, Snapdr	V, 4AU, comm D 205, 29, SD D 636, 2 / SD SD 820, 45 / SD SDM439, 220, _2016	bullet	in				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2279 An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
NULL Pointer Dereferenc e	25-07-2019	7.8	CVE ID : CVE-2019-2281 Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,				https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins		0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	<mark>3-4</mark> 781	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			Snapdr MDM9 MDM9 MSM89 QCS40 215, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63 Snapdr	D 636, SI 2 / SD 71 D 820, SI 5 / SD 85 DM439, 560, SDX 560, SDX	5 in 5 AU, comm D 205, 0, SD 5 D 450, 415, SD 0 665, 0 / SD 0 820A, 50, SD 2 0, 20, 20, 2016					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334 Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

		Description & CVE ID	Patch	NCIIPC ID
		SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
		CVE ID : CVE-2019-2343		
25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1402
		CVE ID : CVE-2019-2345		
25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDM6- 130819/1403
			25-07-20194.4Snapdragon_High_Med_2016, SXR113025-07-20194.4Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24VEY ID : CVE-2019-234525-07-20197.27.27.27.27.27.27.27.27.28889897.27.27.27.28897.2889897.28997.2999<	25-07-20197.2Snapdragon_High_Med_2016, SXR1130Intps://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- connectivity, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin25-07-20194.4Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Vired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660https://ww

	-									
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				783						

Weakness	Publish Date	CVSS	•				Ра	tch	NCIIP	CID
Out-of- bounds Write	22-07-2019	7.5	receive lead to issue in Snapdr Compu Consun Industr Mobile, Music, S in MDM MDM96 MDM96 MDM96 MDM96 MDM96 MDM96 MDM96 MDM96 SD 425 435, SD SD 425 665, SD SD 625 665, SD SD 670 820A, S SDM63 SDX24	write odragon agon ice & arables 06, V, 4AU, comm D 205, 0, SD SD 450, 5, SD SD 710 / 0, SD SD 710 / 0, SD 205, 30 SD 710 / 0, SD 20, 30 20, 50 20, 50 50, 50, 50 50, 50, 50 50, 50, 50, 50, 50, 50, 50, 50, 50, 50,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819			
Use After Free	25-07-2019	4.6	CVE ID : CVE-2019-2287 Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1406
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SDM6- 130819/1407
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	•					tch	NCIIP	C ID
			SDM66	50, SDX2	4					
			CVE ID	: CVE-2	2019-22	93				
Use After Free	25-07-2019	4.6	accessi macro after-fi Snapdi Snapdi Snapdi Snapdi Snapdi MDM9 MDM9 QCS40 212/SI SD 430 625, SI SD 670 845 / S	ompute, onsumer dustrial obile, oice & M earables M9206, M9640, M9640, M8909V 05, SD 22 0 425, S 5, SD 450	info via co use- on Auto, IOT, IOT, usic, s in V, 10/SD D 427, 0, SD SD 710 / OA, SD 4	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819		
Integer Overflow or Wraparou nd	25-07-2019	4.6	trigger comma usersp Snapdn Consur Consur Indust Mobile Music, Infrast in IPQ4 IPQ802 MDM9 MDM9	olied by ication. ito, Snap tronics napdrag Snapdra Snapdra agon Vo igon Win and Net Q8064,	v-crafted a in odragon gon agon oice & red working	https: w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1410
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	O-QUA-SDM6- 130819/1411
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIF	PC ID
			425, SI SD 450 665, SI SD 670 820A, S 850, SI SDM66	4A, 5605, SD 0 435, 5, SD 5D 710 / 0, SD 7 SD 5DM630, 4	bullet	in				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	while h to out o in Snapdr Snapdr Snapdr Snapdr Snapdr Mobile Music, in MDM MDM9 MSM89 QCS40 215, SI SD 425 435, SI SD 615 632, SI SD 712 730, SI SD 845	SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305 Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630,		w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
Integer	25-07-2019	10	Possible integer underflow			https:	//ww	O-QUA-	SDM6-	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 788	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparou nd)			due to lack of validation befor calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835 SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307	ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	130819/1413
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435,	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1414
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24			
			CVE ID : CVE-2019-2308			
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDM6- 130819/1415	
			CVE ID : CVE-2019-2309			
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	O-QUA-SDM6- 130819/1416	
CV Scoring So (CVSS)	cale 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	n & CVE	ID			NCIIP	PC ID
			Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24			bullet	in			
snandragor	1_high_med_20	16 firm	CVE ID	: CVE-2	019-23	12				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So			SDM439			SDA660, 1660,				
(CVSC)	0-1	1-2	2-3	<mark>3-4</mark> 791	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				791						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2235		
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670 SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	mpany/pro duct- security/b ulletins	0-QUA-SNAP- 130819/1418
			CVE ID : CVE-2019-2236		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SNAP- 130819/1419
CV Scoring So (CVSS)	cale 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	D	Ра	tch	NCIIP	CID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9635M, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239							
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605,				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring Sc (CVSS)	cale 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	Descriptio	on & CVE	ID	Ра	tch	NCIIF	PC ID
			Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254 A race condition occurs while							
Use After Free	22-07-2019	6.9	proces can lea conditi Snapdr Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 QCS40 215, SI SD 425 435, SI SD 425 665, SI SD 730 845 / S SDM43 SDX20 Snapdr SXR11	sing per d to a us ion in Sn ragon Co ragon Co ragon Mo ragon Mo ragon W 150, MD 607, MD 607, MD 650, MS 5, QCS60 5, QCS60 5, QCS60 5, SD 427 5, SD 632 5, SD 632 5, SD 632 5, SD 820 5, SD 80 5, SD 8	f-event v se after f apdrago ompute, onsumer dustrial obile, oice & M earables M9206, M9640, M9640, M9640, M9640, M9640, M9640, M9640, SD 212/S 7, SD 430 SD 429, S SD 636 SD 710 / OA, SD 83 SD 855, S30, SDM	which free on Auto, IOT, IOT, usic, s in V, comm D 205, 0, SD SD 450, 5, SD SD 450, 5, SD 2 SD 670, 35, SD 4660, _2016,	w.cod ra.org rity- bullet 19/00	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIP	PC ID
N/A	22-07-2019	4.9	subsys non sec can lea disclos Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Infrast in IPQ8 MDM9 QCA80 215, SI SD 425 435, SI SD 425 435, SI SD 625 650/52 710 / S SD 820 850, SI SDM43 Snapdr	d to info ure in Sr agon Co agon Co agon Co agon Ind agon Mo agon Wi ructure a 3074, ME 206, MD 650, MSI 81, QCS6 0 210/SI 5, SD 427 0 439 / S 5, SD 632 2, SD 632 2, SD 675 50 670, S 60 670, S 60 855, SE 69, SDM6 agon_Hi	LOS or of system is rmation napdrag mpute, nnectivin nsumer dustrial obile, ice & Mi ired and Netwo DM9150 M9607, M8996A 605, Qua D 212/Si 5 D 429, Si 5 SD 430 5 SD 711 5 SD 636 5 SD 711 5 SD 730, Si 5 SD 84 0 8CX, Si 6 30, SDM gh_Med	other memory on Auto, ity, IOT, IOT, usic, working , U, alcomm D 205, 0, SD SD 450, 5, SD 2 / SD SD 820, 45 / SD DA660, 4660, _2016,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263		
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SNAP- 130819/1424
Improper Restriction of Operations within the	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity,	https://ww w.codeauro ra.org/secu rity- bulletin/20	O-QUA-SNAP- 130819/1425
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIP	CID
Bounds of a Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439 SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279	, 19/06/03/ june-2019- code- aurora- security- bulletin		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing car happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SI 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-S 130819/	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SNAP- 130819/1427
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code-	0-QUA-SNAP- 130819/1428
CV Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290	aurora- security- bulletin	
mdm9150_f	firmware				
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MDM9- 130819/1429
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				799						

N/A 25-07-2019 21 12 23 34 45 56 67 78 89 50 820, SD 835, SD 845, SD 865, SD 860, SD 850, SD 860,	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A 25-07-2019 2.1 While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Commute, Snapdragon Consumer IDT, Snapdragon Consumer IDT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM96650, MDM96650, MSM8996AU, QCA6174A, QCA6574AU, QCA6574, QCA6575, SD 211/SD 212/SD 205, SD 425, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 0.4 V CV Scoring Scale 41 12 3.4 4.5 5.6 6.7 7.8 8.4 0.10						
N/A 25-07-2019 2.1 surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics https://ww N/A 25-07-2019 2.1 in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, QCA6574, QCA6564, QCA6574, QCA6574, QCA6574, QCA6574, QCA6574, QCA6574, QCA6574, QCA6574, QCA6574, QCA6574, QCA6574, QCA6570, D 710 / SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820, SD 835, SD 845, SD 820, SD 0-QUA- MDM9-1 130819/1430				CVE ID : CVE-2019-2239		
CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	N/A	25-07-2019	2.1	surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Vired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD	w.qualcom m.com/co mpany/pro duct- security/b	MDM9-
	-	cale 0-1	1-2		6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SXR1130		
			CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/1431
			CVE ID : CVE-2019-2241		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/1432
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253 Position determination							
Informatio n Exposure	25-07-2019	7.5	Positio accurac to wron informa Auto, S Snapdr Snapdr Snapdr Mobile, Music, a in MDM MDM90	n detern cy may b ngly deci ation in napdrag ragon Co ragon Io ragon Io ragon Io ragon Io ragon Io cagon Io cag	nination oded Snapdra on Com nsumer dustrial r, Snapd agon Vo gon We 1DM920 M9615, M9635N M96350, M96350, M96350, SD 210 O 425, SI , SD 210 O 425, SI , SD 210 O 425, SI , SD 439 O 615/10 O 632, SI 665, SD SD 670, A, SD 83 SD 855, S	ded due agon pute, IOT, IOT, lragon ice & arables 06, M, V, V, V, D/SD D 427, 0 / SD D 427, 0 / SD 6/SD D 636, 675, SD 675, SD SD 730, 35, SD	w.qua m.con	n/co y/pro ity/b	0-QUA- MDM9- 130819	
CV Scoring So	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA- MDM9- 130819/1434
			CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/1435
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 803	6-7 7-8	8-9 9-10

Weakness	Publ	ish Date	CVSS	I	Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
				Snapdu Infrast in IPQ& MDM9 QCA80 215, SI SD 425 435, SI SD 625 650/52 710 / S SD 820 850, SI SDM43 Snapdu	Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261						
				Possib proces	le buffer sing the	overflo high lev	w while vel lim				
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-0	7-2019	7.5	improp validat Snapdu Snapdu Snapdu Snapdu Snapdu MDM9 MSM8 ⁴ QCS60 665, SI SD 730 835, SI SDA66	processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130		w.cod ra.org rity- bullet 19/00 june- code- auror	a- ity-	0-QUA- MDM9- 130819	/1436	
Improper Restriction	22-0	7-2019	7.5		y gets u ta and n	pdated nay lead	-	://ww leauro	0-QUA- MDM9-		
CV Scoring So (CVSS)	cale	0-1	1-2	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	NCIIP	CID
of Operations within the Bounds of a Memory Buffer			to access beyond the a memory. in Snapdrago Snapdragon Connectiv Snapdragon Consume Snapdragon Industria Snapdragon Mobile, Snapdragon Voice & M Snapdragon Wearable MDM9150, MDM9607 MDM9650, MSM8909 MSM8996AU, QCA657 QCS405, QCS605, Qua 215, SD 210/SD 212/S SD 425, SD 439 / SD 4 450, SD 625, SD 632, S SD 665, SD 675, SD 71 710 / SD 670, SD 730, SD 820A, SD 835, SD 8 850, SD 855, SDA660, SD SDX24, Snapdragon_High_Med CVE ID : CVE-2019-2	on Auto, 1 rity, 1 r IOT, 1 I IOT	ra.org/s rity- bulletin 19/06/ june-20 code- aurora- security bulletin	n/20 /03/)19- - y-	130819	/1437
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferer happen when playing with wrong block grou Snapdragon Auto, Sna Compute, Snapdragon Consumer IOT, Snapdr Industrial IOT, Snapdr IoT, Snapdragon Mobi Snapdragon Voice & M Snapdragon Wearable MDM9150, MDM9206 MDM9607, MDM9650 MSM8909W, MSM899 QCS405, QCS605, Qua 215, SD 210/SD 212/S SD 425, SD 427, SD 43 435, SD 439 / SD 429, SD 600, SD 615/16/SI	the clip up id in pdragon ragon le, lusic, s in 6AU, comm SD 205, 0, SD SD 450,	https:// w.qualc m.com/ mpany/ duct- security ulletins	com /co /pro y/b	O-QUA- MDM9- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	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
			625, SD 632, SD 6 SD 675, SD 712 / 670, SD 730, SD 8 SD 835, SD 845 / 855, SDA660, SDI SDM630, SDM660 Snapdragon_High	SD 710 / SD 20, SD 820A, SD 850, SD M439, 0, SDX20, _Med_2016				
Out-of- bounds Write	22-07-2019	7.5	Improper validat received from firm lead to an out of k issue in video dri Snapdragon Auto Compute, Snapdr Consumer IOT, Sm Industrial IOT, Sm Mobile, Snapdrag Music, Snapdrag Music, Snapdrag Music, Snapdrag MDM9607, MDM MDM9650, MSM MSM8996AU, QC QCS405, QCS605, 215, SD 210/SD 2 SD 425, SD 427, S 435, SD 439 / SD SD 625, SD 632, S 665, SD 675, SD 7 SD 670, SD 730, S 820A, SD 835, SD 850, SD 855, SDA SDM630, SDM660 SDX24 CVE ID : CVE-20	mware can bound write ver. in , Snapdragon agon hapdragon apdragon on Voice & on Wearables M9206, 9640, 3909W, A6574AU, Qualcomm 212/SD 205, 5D 430, SD 429, SD 450, 5D 636, SD 12 / SD 710 / 5D 820, SD 845 / SD 660, SDM439, 0, SDX20,	https: w.cod ra.org rity- bullet 19/06 june-2 code- aurora securi bullet	eauro /secu in/20 6/03/ 2019- a- ty-	0-QUA- MDM9- 130819	
Improper Restriction of Operations within the Bounds of	22-07-2019	4.6	Out of bound acco due to buffer cop checking size of in from WLAN firmy Snapdragon Auto Consumer IOT, Sn	https: w.cod ra.org rity- bullet 19/06	eauro /secu in/20	O-QUA- MDM9- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292		
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MDM9- 130819/1441
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20	O-QUA- MDM9- 130819/1442
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 807	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
			Connec Consum Industr Mobile, Music, S Infrastr in IPQ4 IPQ807 MDM92 MDM92 MDM92 MDM92 MDM92 MDM92 SD210 425, SE SD 450 636, SE SD 670 820A, S 850, SE SDX24	4019, IP(74, MDM 206, MD 640, MD 996AU, Q 74AU, Q 77, QCA 0/SD 212 0 427, SE 0, SD 600 0 675, SE 0, SD 730 SD 835, SE	napdrag Snapdra Snapdra agon Vo agon Wir and Netv Q8064, 19150, M9607, M9650, QCA6174 (CA8081 9379, Q0 2/SD 205 D 430, SI 0, SD 625 D 712 / S 0, SD 820 SD 845 / DM660, S	agon agon bice & red working 4A, 5, SD 5, SD 0 435, 5, SD 5, SD SD 710 / 0, SD / SD SDX20,	19/07 july-2 code- auror securi bullet	a- ity-		
Out-of- bounds Read	25-07-2019	7.5	CVE ID : CVE-2019-2299 Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD				w.cod ra.org rity- bullet	a- ity-	0-QUA- MDM9- 130819	
			SD 450	, SD 625	5, SD 636	5, SD				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2305		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA- MDM9- 130819/1444
			Possible integer underflow	https://ww	
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	nttps://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-	O-QUA- MDM9- 130819/1445
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIF	PC ID
			Snapdr MDM9 MDM9 QCA61 QCA93 QCS60 205, SI SD 435 625, SI SD 712 730, SI SD 845 SDM63 SDX24		vice & M M9206, M9640, M8996A A6574A 9379, Q 0/SD 21 0 /SD 21 0 /SD 600 0 /SD 600 0 665, SI 0 / SD 60 0 820A, 1 0, SD 85 560, SDX	U, U, CS405, 2/SD 0 430, 0, SD 0 675, 70, SD SD 835, 55, 20,	secur			
N/A	25-07-2019	7.2					w.cod ra.org rity- bullet	a- ity-	0-QUA- MDM9- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

1-2	2-3	3-4	4-5	5-0	6-7	
		810				

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCIIF	PC ID
			CVE ID : CVE-2019-2308							
Out-of- bounds Read	25-07-2019	7.5	from fi integer since d exceed Snapdr Consur Consur Industr Mobile Music i MDM9 MDM9 MDM9 MSM89 QCA65 QCA93 205, SI SD 712 820A, S	storing c rmware overflo ata leng real dat ragon Au ner Elec ctivity, S ner IOT, rial IOT, , Snapdr in MDM9 206, MD 640, MD 640, MD 640, MD 996AU, Q 74AU, Q 74AU, Q 79, SD 2 0 425, SI 2 / SD 71 SD 845 / 50, SDX2 0 : CVE-2	in cache w may o th receiv a length ito, Snap tronics napdrag Snapdra Snapdra agon Vo 9150, M9607, M9650, QCA6174 CA9377 10/SD 2 0 625, SI 0 / SD 6 SD 850 0	e, An occur ved may . in odragon agon agon ice & 4A, , 212/SD 0 636, , 70, SD	w.cod ra.org rity- bullet	a- ity-	0-QUA- MDM9- 130819	
mdm9640_1	firmware						1		1	
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M,				w.qua m.con	n/co y/pro ity/b	0-QUA- MDM9- 130819	
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIP	PC ID
			SXR11							
N/A	25-07-2019	2.1	Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239 While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574,				w.qua m.cor	n/co y/pro ity/b	0-QUA- MDM9- 130819	
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130		
			CVE ID : CVE-2019-2240		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDX20, Snapdragon_High_Med_2016,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/1450

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				813						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/1451
Use After Free	25-07-2019	4.6	CVE ID : CVE-2019-2260 Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/1452
CV Scoring So (CVSS)	cale 0-1	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	NCIIF	C ID
			MDM9206, MDM MDM9640, MDM MSM8909W, MS QCA9531, QCA9 210/SD 212/SD SD 427, SD 430, 450, SD 625, SD 650/52, SD 712 670, SD 820, SD SD 845 / SD 850 SDX20, Snapdragon_Hig CVE ID : CVE-20	M9650, SM8996AU, 9980, SD 205, SD 425, SD 435, SD 636, SD 4 / SD 710 / SD 820A, SD 835, 0, SDM660, gh_Med_2016				
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer der occurs for chann while opening g Snapdragon Aut Consumer IOT, S Mobile, Snapdrag in MDM9607, M MSM8909W, QC SD 425, SD 427, 435, SD 439 / S SD 625, SD 632, 712 / SD 710 / S 820A, SD 835, S 850, SDM439, S SDM660, SDX24 CVE ID : CVE-20	https: w.cod ra.org rity- bullet 19/06 june-2 code- aurora securi bullet	eauro /secu in/20 5/03/ 2019- a- ty-	0-QUA- MDM9- 130819		
Improper Authentica tion	25-07-2019	7.2	User keystore si ignored in boot bypass boot ima verification in S Auto, Snapdrago IOT, Snapdrago MDM9607, MDM SD 427, SD 430, 450, SD 625, SD SD 710 / SD 670	https: w.cod ra.org rity- bullet 19/07 july-2 code- aurora securi	eauro /secu in/20 7/01/ 019- a-	0-QUA- MDM9- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SDM660	bulletin	
			CVE ID : CVE-2019-2278		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA- MDM9- 130819/1455
			CVE ID : CVE-2019-2287 Multiple open and close from	https://ww	
Use After Free	25-07-2019	4.6	multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650,	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/1456
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016		
			CVE ID : CVE-2019-2290		
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MDM9- 130819/1457
			CVE ID : CVE-2019-2298		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	O-QUA- MDM9- 130819/1458
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24	bulletin	
Out-of- bounds Read	25-07-2019	7.5	CVE ID : CVE-2019-2299 Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MDM9- 130819/1459

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
818										

Out-of- bounds Read25-07-2019ZZSDM660, SDX20, SDX24 CVE ID : CVE-2019-23050ut-of- bounds Read25-07-2019IVPossible integer underflow due to lack of validation before calculation of data length n 802.11 Rx management configuration in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Auto, Snapdragon Readhttps://ww w.codeauro ra.org/secu rity- bulletin0ut-of- bounds Read25-07-20197.5To Ever-2019-2307https://ww w.codeauro ra.org/secu rity- bulletin/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/20 NoBelein/	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds25-07-20197.5Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, MDM9150, MDM9026, MDM9607, MDM96640, Uderflow (Wrap or M1)https://ww w.codeauro rity- bulletin/20 0-QUA- MDM9650, MSM8996AU, Ig/07/01/ MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6377, QCA9377, QC4057, D25, SD 425, SD 427, SD 430, SD 435, SD 435, SD 430, SD 660, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 855, SD 845 / SD 850, SD 857, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 845 / SD 850, SD 856, SD 856, SD 845 / SD 850, SD 856, SD 845 / SD 85				SDM660, SDX20, SDX24		
Out-of- bounds25-07-20197.5While storing calibrated data from firmware in cache, An integer overflow may occur snapdragon Auto, Snapdragonhttps://ww w.codeauro ra.org/secu rity- bulletin0-QUA- MDM9-60 MDM9-60, MDM9-60, MDM9406, bulletin/200ut-of- bounds25-07-20197.5While storing calibrated data from firmware in cache, An integer overflow may occur snapdragon Auto, Snapdragon0-QUA- MDM9-60, MDM9-60, pulletin/200ut-of- bounds25-07-20197.5While storing calibrated data from firmware in cache, An integer overflow may occur snapdragon Auto, Snapdragonhttps://ww w.codeauro ra.org/secu rity- bulletin0ut-of- bounds25-07-20197.5While storing calibrated data from firmware in cache, An integer overflow may occur snapdragon Auto, Snapdragonhttps://ww w.codeauro ra.org/secu rity- bulletin0ut-of- bounds25-07-20197.5While storing calibrated data from firmware in cache, An integer overflow may occur snapdragon Auto, Snapdragonhttps://ww w.codeauro ra.org/secu rity- bulletin/100ut-of- bounds25-07-20197.5Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & ww.codeauro snapdragon findustrial IOT, Snapdragonhttps://ww w.codeauro ra.org/secu rity- bulletin/200ut-of- bounds25-07-20197.5While storing calibrated data from firmware in cache, An integer overflow may occur sceud rity- bulletin in Snapdragon Poloce & aurora- security- bulletin/20https://ww w.codeauro ra.org/secu rity- <td></td> <td></td> <td></td> <td>CVE ID : CVE-2019-2305</td> <td></td> <td></td>				CVE ID : CVE-2019-2305		
Out-of- bounds Read25-07-20197.5While storing calibrated data from firmware in cache, An 	Underflow (Wrap or Wraparou	25-07-2019	10	due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	MDM9-
	bounds Read		7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	MDM9-

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pat	tch	NCIIP	CID
			MDM9 MDM9 MSM89 QCA65 QCA93 205, SI SD 712 820A, S SDM66 CVE ID							
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, D212/SD 205, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312			w.cod ra.org rity-	019- a- ity-	0-QUA- MDM9- 130819		
msm8909w	_firmware									
Improper Restriction of Operations within the	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto,				https: w.qua m.con mpan duct-	n/co	0-QUA- MSM8- 130819	
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	C ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243				secur	• •		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD				w.qua m.con	n/co y/pro ity/b	0-QUA- MSM8- 130819	/1464
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA- MSM8- 130819/1465
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/	O-QUA- MSM8- 130819/1466
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670 SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260	june-2019- code- aurora- security- bulletin	
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835,	https://ww w.codeauro ra.org/secu rity- bulletin/20	0-QUA- MSM8- 130819/1467
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016		
NULL Pointer Dereferenc e	22-07-2019	4.6	CVE ID : CVE-2019-2263 Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA- MSM8- 130819/1468
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MSM8- 130819/1469
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID		Pa	tch	NCIIF	PC ID		
			CVE ID	: CVE-2	019-22	72				
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273		w.qua m.con	n/co y/pro ity/b	0-QUA- MSM8- 130819			
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636,		w.cod ra.org rity- bullet	a- ity-	0-QUA- MSM8- 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

0-1	1-2	2-3	3-4	4-5	5-6	6-7	
			825				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MSM8- 130819/1472
Improper Restriction of Operations within the Bounds of	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b	O-QUA- MSM8- 130819/1473
CV Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343	ulletins	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2345	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MSM8- 130819/1474
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in	https://ww w.codeauro ra.org/secu rity-	O-QUA- MSM8- 130819/1475
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 , SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439 SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287	19/06/03/ june-2019- code- aurora- security- bulletin	
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA- MSM8- 130819/1476
			820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016		
			CVE ID : CVE-2019-2290		
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA- MSM8- 130819/1477
			CVE ID : CVE-2019-2293		
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA- MSM8- 130819/1478

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				829						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA- MSM8- 130819/1479
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA- MSM8- 130819/1480
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Ра	tch	NCIIP	CID
			SDM66	SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306						
N/A	25-07-2019	7.2	CVE ID : CVE-2019-2306User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer 				w.cod ra.org rity- bullet	a- ity-	0-QUA- MSM8- 130819	
qcs605_firm	nware	1					T			
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	-
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			in MDM MDM99 MSM89 QCS609 410/12 430, SE SD 450 636, SE SD 820 845 / S SDM43 Snapdr SXR113	working)7, 5, SD 7, SD 5D 429, 2, SD 5D 670, 35, SD SDA660, 4660, _2016,						
			CVE ID) : CVE-2	019-22	35				
NULL Pointer Dereferenc e	25-07-2019	2.1	during termina applica Auto, S Snapdr	ointer de secure a ation usi ation ids. Snapdrag ragon Co ragon Co ragon Co ragon Co ragon Mo ragon Mo ragon Wi ructure a 3074, ME 607, MD 655, MSI 81, QCS6 0 410/12 0 430, SE 0 50 450 0 636, SE 0 712 / S 0 8CX, SE	applicati ing spec in Snap gon Com nnectivit nsumer dustrial obile, ired and Netv DM9206 M9650, M8996A 505, Qua 2, SD 422 D 435, SI 0, SD 625 D 650/52 SD 710 / D, SD 820	on ific odragon pute, ity, IOT, IOT, IOT, usic, working , U, alcomm 5, SD D 439 / 5, SD 2, SD 2, SD	w.qua m.cor mpan duct- secur ulletin	n/co y/pro ity/b	0-QUA- 130819	٠

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2236		
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS6- 130819/1484
Out-of- bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS6- 130819/1485
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130		
			CVE ID : CVE-2019-2238		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS6- 130819/1486
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly	https://ww w.qualcom m.com/co	0-QUA-QCS6- 130819/1487
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 834	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			unpred Snapdr Compu Connec Consur Industr IoT, Sna Snapdr Infrastr in IPQ4 IPQ807 MDM92 QCA65 QCA5 QCA5 QCA5 QCA5 QCA5 QCA5 QCA5 QCA	019, IP(4, MDM 206, MD 640, MD 96AU, Q 64, QCA 74AU, Q 84AU, Q 77, QCA 80, QCA 80, QCA 730, SI , SD 712 600, SI , SD 712 730, SI , SD 845 86X, SI 0, SDM6 5XR113 : CVE-2	behaviou ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra ired and Netw 28064, 9150, M9607, M9650, QCA6174 6574, CA6584 CA8081 9379, QC 9886, QC 404, QCS 2/SD 205 2/SD 205 2/SD 205 2/SD 205 2/SD 71 2/SD 71	dragon on agon gon e, isic, working AA, A, CA9531, CA9531, CA9980, 5605, 5, SD 0 636, 0 / SD 0 636, 0 / SD 0 820A, 0, SD 0 820A, 0, SD	duct- secur ulletin	ns		
Improper Input Validation	25-07-2019	2.1	backgro check is and als handlir to unin in Snap	renderin ound, Er s not cau o incorr ng is bein tended S odragon ragon Co	rror stati ught pro ect statu ng done SUI beha Auto,	us perly Is leading	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	-
CV Scoring Sc	cale 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	Ра	tch	NCIIP	CID
			Snapdr Snapdr Electro Snapdr Snapdr Snapdr Infrast in MDM MDM9 QCS40 212/SI 636, SI SD 670 820A, S 850, SI SDM63 SXR11							
				e buffer						
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835,				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring Sc (CVSS)	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660		
			CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS6- 130819/1490
Informatio n Exposure CV Scoring So	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS6- 130819/1491
(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	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			MDM99 MDM99 MDM99 MDM99 MSM89 Qualco 212/SI SD 430 429, SI 415, SI SD 650 712 / S SD 820 845 / S SDA66 SDA66 Snapdr SXR113							
			CVE ID	: CVE-2	019-22	54				
Use After Free	22-07-2019	6.9	CVE ID : CVE-2019-2254 A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	v
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS6- 130819/1493
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019-	0-QUA-QCS6- 130819/1494
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE	ID	Patch	NCIIP	'C ID
			in MDM9607, MDM964 MSM8909W, QCS405, SD 425, SD 427, SD 439 435, SD 439 / SD 429, SD 625, SD 632, SD 630 712 / SD 710 / SD 670 820A, SD 835, SD 845, 850, SDM439, SDM630 SDM660, SDX24 CVE ID : CVE-2019-22	QCS605, aur), SD sec SD 450, bul 6, SD , SD / SD),	de- rora- curity- lletin		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflo processing the high lev process action frame d improper buffer length validation in Snapdrag Snapdragon Compute, Snapdragon Consumer Snapdragon Industrial Snapdragon Mobile, Snapdragon Voice & M MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 63 665, SD 712 / SD 710 / SD 730, SD 820, SD 820, SDA660, SDM630, SDM SDX20, SDX24, SXR113 CVE ID : CVE-2019-22	vel lim ue to on Auto, i OT, IOT, IOT, i IOT, i IOT, IIOT, i IOT, IIII IOT, IIIII IOT, IIIIII IOT, IIIIII IOT, IIIIII IOT, IIIIIII IIIIII IIIIII IIIIII IIIIII IIII	lletin/20 /06/03/ ne-2019-	0-QUA- 130819	-
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault whi playing h265 video file denial of service issue Snapdragon Auto, Snap Compute, Snapdragon Connectivity, Snapdrag Consumer IOT, Snapdr Industrial IOT, Snapdr Mobile, Snapdragon Vo Music, Snapdragon We in MSM8909W, QCS60	e leads to in http odragon w.c gon mp agon duo agon sec oice & ulle	ps://ww qualcom com/co oany/pro ct- curity/b etins	0-QUA- 130819	
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730 SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2273		
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCS6- 130819/1497
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora-	0-QUA-QCS6- 130819/1498
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descripti	on & CVE ID		Pat	ch	NCIIF	C ID
			MSM8996AU, QCS605, SD 21 205, SD 425, S SD 435, SD 425, S 636, SD 665, S SD 710 / SD 67 820A, SD 835, 850, SD 855, S SDM660, SDX2 CVE ID : CVE-2	10/SD 212/3 D 427, SD 4 0, SD 625, S D 675, SD 7 70, SD 730, SD 845 / SI DA660, SDN 24	30, D 12 / SD D M630,	securi bulleti			
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory with invalid da to access beyo memory. in Sm Snapdragon Co Snapdragon Co Snapdragon M Snapdragon M Snapdragon W MDM9150, MI MDM9650, MS MSM8996AU, QCS405, QCS6 215, SD 210/S SD 425, SD 439 450, SD 625, S SD 665, SD 675 710 / SD 670, SD 820A, SD 8 850, SD 855, S SDM630, SDM SDX24, Snapdragon_H CVE ID : CVE-2	ata and may nd the alloc apdragon A onnectivity, onsumer IO dustrial IO dustrial IO dobile, oice & Musi Vearables in DM9607, SM8909W, QCA6574AI 05, Qualcon D 212/SD 2 9 / SD 429, D 632, SD 6 5, SD 712 / SD 730, SD 35, SD 845, DA660, SDX20 (igh_Med_20)	v lead cated Auto, , T, T, T, c, , v , v , v , v , v , v , v , v , v	https:/ w.code ra.org/ rity- bulleti 19/06 june-2 code- aurora securi bulleti	eauro /secu in/20 /03/ 2019- a- ty-	0-QUA- 130819	
Improper Restriction of Operations	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified			https:, w.qua m.com mpany	lcom n/co	0-QUA- 130819	•
within the			code. in Snapd	ragon Comj	pute,	duct-			
CV Scoring So	cale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2281	security/b ulletins	
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-QCS6- 130819/1501
Improper Restriction	25-07-2019	2.1	Out of bound read and information disclosure in	https://ww w.qualcom	0-QUA-QCS6- 130819/1502
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 843	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343	m.com/co mpany/pro duct- security/b ulletins	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2345	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCS6- 130819/1503
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820 SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346	duct- security/b ulletins	0-QUA-QCS6- 130819/1504
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-QCS6- 130819/1505
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			850, SE SDM63 SDX24	0 855, SI 0, SDM6	560, SDX	SDM439, 20,				
					2019-22					
Use After Free	25-07-2019	4.6	multipl camera destroy in Snapdr Snapdr Snapdr Snapdr Snapdr MDM92 MDM92 MDM94 QCS603 430, SE SD 636 SD 710 820A, SE 850, SE	e thread driver f ved sess odragon Co agon Co agon Mo agon M 206, MD 640, MD 640, MD 640, MD 640, MD 640, SD 65, SD 42 0 435, SI , SD 650 / SD 67 50 835, S 0M660, S	Auto, onnectiv onsumer dustrial	ead s pointer ity, 10T, 10T, 10T, 5 in 6AU, 7, SD 0 625, 712 / 20, SD / SD 5DX24,	w.cod ra.org rity-	019- a- ity-	0-QUA- 130819	-
					2019-22					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD			w.cod ra.org rity-	2019- a- ity-	0-QUA- 130819	-	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2292		
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2293	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCS6- 130819/1508
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-QCS6- 130819/1509
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			845 / SD 850, SD 855, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2298		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCS6- 130819/1510
Improper			Possibility of out-of-bound	https://ww	
Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-	0-QUA-QCS6- 130819/1511
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 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 IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301	security- bulletin	
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCS6- 130819/1512
Improper Restriction of Operations within the Bounds of	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/	0-QUA-QCS6- 130819/1513
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC II	D
a Memory Buffer			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306	july-2019- code- aurora- security- bulletin		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QC 130819/1	
CV Scoring So			2-3 3-4 4-5 5-6	6-7 7-8		9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2307		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCS6- 130819/1515
			CVE ID : CVE-2019-2308		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-QCS6- 130819/1516
CV Scoring So (CVSS)	cale 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	on & CVE	ID	Ра	tch	NCIIP	CID
			QCA61 QCA93 QCS60 205, SI SD 435 625, SI SD 712 730, SI SD 845 SDM63	640, MS 74A, QC 77, QCA 5, SD 21 0 425, SI 0 425, SI 0 636, SI 2 / SD 450 0 636, SI 2 / SD 71 0 820, SI 6 / SD 85 80, SDM6 0 : CVE-2	A6574A 9379, Q 0/SD 21 0 427, SI 0, SD 600 0 665, SI 0 / SD 6 0 820A, S 560, SDX	U, CS405, 2/SD D 430, 0, SD D 675, 570, SD SD 835, 55, (24				
sd_670_firm	iware									
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	emulat sector TA roll Snapdu Compu Connee Consur Indust Mobile Music, Infrast in MDM MDM9 MSM89 QCS60 410/12 430, SI SD 450 636, SI SD 820 845 / S	ragon Au ite, Snap ctivity, S ner Elec ctivity, S ner IOT, rial IOT, , Snapdr Snapdra ructure 49206, N 650, MD 996AU, C 5, Qualco 2, SD 42! 0, SD 625 0, SD 625 0, SD 850, S 89, SDM6 ragon_Hi	B is used imption otection ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra (Snapdra Snapdra Snapdra (Snapdra Snapdra (Snapdra Snapdra (Snapdra Snapdra (Snapdra	d due to s in the logic. in odragon gon agon oice & ced working 07, 5, SD 7, SD 5, SD 7, SD 5D 429, 2, SD 5D 670, 35, SD 5D 670, 35, SD	w.qua m.cor mpan duct- secur ulletin	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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-2019-2235		
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1518
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_6- 130819/1519
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237		
Out-of- bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2238	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1520
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_6- 130819/1521
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 854	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIF	PC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9635M, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239				
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150,	https: w.qua m.com mpany duct- securi ulletir	lcom n/co y/pro	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 /	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_6- 130819/1523
CV Scoring So	cale 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	Pa	tch	NCIIP	PC ID
			820A, SD 835, 850, SD 855, SI SDM630, SDM6 SXR1130	D 8CX, SDA660,				
			CVE ID : CVE-2	2019-2241				
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	end of iterating getting the ver lead to informa in Snapdragon Co Snapdragon Co Snapdragon Io Snapdragon Io Mobile, Snapdra Music, Snapdra in MDM9206, M MDM9650, MS MSM8996AU, O 210/SD 212/S SD 427, SD 430 439 / SD 429, S 615/16/SD 41 632, SD 636, SI SD 712 / SD 71	sion info and ation disclosure. Auto, ompute, onsumer IOT, dustrial IOT, T, Snapdragon ragon Voice & agon Wearables MDM9607, M8909W, QCS605, SD D 205, SD 425, D 205, SD 425, SD 435, SD SD 450, SD 5, SD 625, SD 5, SD 625, SD 0 665, SD 675, 0 / SD 670, SD D 820A, SD 835, 50, SD 855, 39, SDM630,	https: w.qua m.con mpan duct- securi ulletin	n/co y/pro ity/b	0-QUA- 130819	
Improper Input Validation	25-07-2019	7.5	Buffer over-rea while parsing a corrupted com Snapdragon Au Connectivity, S Consumer IOT, Industrial IOT, IoT, Snapdragon Vo Snapdragon W	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins		0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pat	tch	NCIIP	CID
			MDM96 MSM89 QCS409 215, SE SD 425 435, SE SD 600 625, SE SD 675 670, SE SD 835 855, SE SDM63	150, MD 607, MD 909W, M 5, QCS60 9 210/SI 9 210/SI 9 30 427 9 439 / S 9 50 427 9 50 427 9 50 427 9 50 51 9 50 845 9 6 50 8 9 5 6 9 5 6 9 5 6 9 5 6 9 5 7 9 5 7	M9650, SM8996)5, Qualo) 212/S , SD 430 SD 429, S /16/SD) 636, SI / SD 71) 820, SI / SD 85 DM439, 560, SDX	5AU, comm D 205, 0, SD 5D 450, 415, SD D 665, 0 / SD D 820A, 50, SD				
Informatio n Exposure	25-07-2019	7.5	Positio accurat to wron informa Auto, S Snapdr Snapdr Snapdr Mobile, Music, a in MDM MDM90	n detern cy may b ngly deca ation in a napdrag ragon Co ragon Io ragon So ragon Io ragon Io r	nination e degra oded Snapdra gon Com nsumer dustrial F, Snapd agon Vo gon We (DM920 M9615, M9635N M9650, M9650, M8909V QCS605, SD 210 O 425, SI , SD 210 O 425, SI (SD 210 O 615/10 O 632, SI 665, SD SD 670, A, SD 83	ded due agon pute, IOT, IOT, Iragon ice & arables 06, 4, V, V, 0/SD 0 427, 0 / SD 0 427, 0 / SD 0 427, 0 / SD 0 636, 675, SD 675, SD . SD 730, 35, SD	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
			SDA66	0, SDM4	39. SDM	[630.				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1527
			CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1528
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 859	6-7 7-8	8-9 9-10

Free 25-07-2019 4.6 in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 130819/152	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free25-07-20194.6happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wiredhttps://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin0-QUA-SD_6 130819/152				Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
450, SD 825, SD 836, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660,		25-07-2019	4.6	happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835,	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	0-QUA-SD_6- 130819/1529
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1	-	cale 0-1	1-2	2-3 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, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263		
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_6- 130819/1530
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_6- 130819/1531

	CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
L					861						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_6- 130819/1532
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_6- 130819/1533

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
862										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			SXR1130			
			CVE ID : CVE-2019-2273			
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1534	
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1535	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID			Pa	tch	NCIIPC ID		
			CVE ID : CVE-2019-2277							
Improper Authentica tion	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 CVE ID : CVE-2019-2278				w.cod	7/01/ 019- a- ity-	0-QUA-SD_6- 130819/1536	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279				w.cod ra.org rity-	2019- a- ity-	0-QUA- 130819	
Improper Restriction	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to			https: w.qua	//ww lcom	O-QUA-SD_6-		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2281	m.com/co mpany/pro duct- security/b ulletins	130819/1538
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1539

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				865						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2334		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1540
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1541

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				066						

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			SDM66	0, SDX2	0, SDA6 0, SDX2	4				
			CVE ID	: CVE-2	019-23	45				
Improper Validation of Array Index	25-07-2019	7.2	of over scan co host be validat Compu Consur Industr Mobile Music, Infrastr in IPQ8 QCS40- 425, SI SD 450 712 / S SD 835 855, SI SDM63	writing mmand cause o ion. in S te, Snap ner IOT, rial IOT, , Snapdr Snapdra ructure 3074, QC 4, QCS4(0 427, SI , SD 625 5D 710 / , SD 845 0 8CX, SI 0, SDM6	Snapdr Snapdra agon Vo gon Win and Net A8081, 05, QCS6 0 430, SI 5, SD 636 SD 670, 5 / SD 85 0A660,	y when a from per gon agon agon oice & red working 505, SD D 435, 5, SD 5, SD 5, SD 5, SD 5, SD 5, SD 5, SD	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
Out-of- bounds Write	22-07-2019	7.5	receive lead to issue ir Snapdr Compu Consur Industr Mobile Music, in MDM MDM9 MSM89 QCS40 215, SI	ed from f an out c a video c ragon Au te, Snap ner IOT, rial IOT, Snapdr Snapdra (19150, M 650, MS 650, MS 996AU, (5, QCS6(0 210/S)	firmwar of bound Iriver. ir Ito, Snar	l write h odragon agon agon bice & arables 06, V, 4AU, comm D 205,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2287		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_6- 130819/1544
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security-	0-QUA-SD_6- 130819/1545
CV Scoring So (CVSS)	cale 0-1	1-2	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
			QCA6574AU, QCS SD 210/SD 212/S 425, SD 427, SD 4 SD 450, SD 625, S 665, SD 712 / SD SD 730, SD 820A, 845 / SD 850, SD SDM630, SDM660 SDX24 CVE ID : CVE-20	SD 205, SD 430, SD 435, 5D 636, SD 710 / SD 670, 5D 835, SD 855, SDA660, 0, SDX20,	bullet	in		
Use After Free	25-07-2019	4.6	Pointer dereferer freeing IFE resou lack of length che resource. in Snap Consumer IOT, Sr Industrial IOT, Sr Mobile, Snapdrag Music, Snapdrag Music, Snapdrag QCS605, SD 425, 430, SD 435, SD 4 SD 636, SD 675, S 710 / SD 670, SD SD 850, SD 855, S SDM660, SDX24 CVE ID : CVE-20	rces due to eck of in port dragon napdragon apdragon gon Voice & on Wearables QCS405, SD 427, SD 450, SD 625, SD 712 / SD 730, SD 845 / SDM630,	https: w.cod ra.org rity- bullet 19/07 july-2 code- aurora securi bullet	eauro /secu in/20 7/01/ 019- a- ty-	0-QUA- 130819	
Use After Free	25-07-2019	4.6	Protection is miss accessing md sess macro which can after-free in Snap Snapdragon Com Snapdragon Cons Snapdragon Indu Snapdragon Mob Snapdragon Woic Snapdragon Wea MDM9150, MDM MDM9607, MDM MDM9650, MSM8 QCS405, QCS605,	sions info via lead to use- odragon Auto, pute, sumer IOT, strial IOT, ile, e & Music, rables in 9206, 9640, 3909W,	https: w.qua m.con mpany duct- securi ulletir	lcom 1/co y/pro ty/b	0-QUA- 130819	
CV Scoring So	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)			869					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427 SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24	0 /	
			CVE ID : CVE-2019-2298		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-craft command supplied by a userspace application. in Snapdragon Auto, Snapdrago Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networki in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605 SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20 SDX24 CVE ID : CVE-2019-2299	ed https://ww https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1548
Improper Restriction of Operations within the	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdrago Compute, Snapdragon	ra.org/secu	0-QUA-SD_6- 130819/1549
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 870	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301	19/07/01/ july-2019- code- aurora- security- bulletin	
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1550
Improper Restriction	25-07-2019	4.6	Improper casting of structure while handling the buffer leads	https://ww w.codeauro	0-QUA-SD_6- 130819/1551
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 871	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
of Operations within the Bounds of a Memory Buffer			in Snap Snapdr Snapdr Snapdr Snapdr Mobile Music, in MDM MDM90 MSM89 QCS409 215, SE SD 425 435, SE SD 425 435, SE SD 425 435, SE SD 615 632, SE SD 712 730, SE SD 845 SDA660 SDM66	of bound odragon 1 agon Co agon Co agon Ind agon Io agon Io Io Io Io Io Io Io Io Io Io Io Io Io I	Auto, nnectivi nsumer dustrial Γ, Snapd agon Vo gon We (DM920 M9650, SM8996 D5, Qualo D5, Qualo D5, Qualo D5, Qualo D5, Qualo D5, Qualo D665, SI 0 429, S 415, SD D665, SI 0 / SD 6 D820A, S 0, SD 85 39, SDM 0	ty, IOT, IOT, ragon ice & arables 6, 5AU, comm D 205, 0, SD 5D 450, 625, SD 0 675, 70, SD 5D 835, 5, 630,	rity-	019- a- ity-		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	due to i calcula 802.11 configu Auto, S Electro Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 QCA61 QCA63 QCS60	e integer lack of v tion of d Rx man tration in napdrag onics Con ragon Co ragon Co ragon Mo agon Mo 650, MD 650, MD 650, MSI 74A, QCA 77, QCA 5, SD 210	alidation ata leng agemen n Snapdi on Cons nectivit nsumer dustrial obile, ice & Mu M9206, M9640, M8996A A6574A 9379, Q0	n before th in t ragon tumer y, IOT, IOT, LOT, usic in U, U, U, CS405, 2/SD	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2307		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1553
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code-	0-QUA-SD_6- 130819/1554
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2309 When handling the vendor command there exists a potential buffer overflow due to lack of input validation of	aurora- security- bulletin	
			command there exists a potential buffer overflow due to lack of input validation of		
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-2019	4.6	data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_6- 130819/1555

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				97/						

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
NULL Pointer Dereferenc e	25-07-2019	2.1	during termin applica Auto, S Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Infrastr in IPQ& MDM9 QCA80 215, SI 427, SI 427, SI 5D 429 632, SI 5D 730 835, SI SDM43 Snapdr), SD 820 D 8CX, SI 89, SDM6 ragon_Hi 30	applicati ing spec in Snap on Com nnectivit nsumer nectivit nsumer dustrial obile, ice & Mi obile, ice & Mi ob	on ific odragon pute, ity, ity, IOT, IOT, usic, working , U, alcomm 5, SD 2, SD 2, SD 2, SD 2, SD 5, SD 2, SD 3, SD 2, SD 439 / 5, SD 2, SD 3, SD 439 / 5, SD 2, SD 3, SD 4, SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
N/A	25-07-2019	2.1	CVE ID : CVE-2019-2236 Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	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 in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130		
			CVE ID : CVE-2019-2237		
Out-of- bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2238	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1558
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1559
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIF	PC ID
			Infrast in MDM MDM9 MDM9 QCS40 215, SI SD 410 430, SI SD 450 625, SI 650/52 710 / S SD 820 850, SI SDM43 SDX20 Snapdi SXR11		and Net MDM920 M96351 M9650, M8996A D5, Qual D 212/S 425, SD D 439 / S 5/16/SD D 636, SI 5, SD 71 SD 730, S 35, SD 84 DA660, 530, SDM					
N/A	25-07-2019	2.1	CVE ID : CVE-2019-2239While sending the renderedsurface content to the screen,Error handling is not properlychecked results in anunpredictable behaviour inSnapdragon Auto, SnapdragonCompute, SnapdragonConnectivity, SnapdragonConsumer ElectronicsConsumer IOT, SnapdragonIndustrial IOT, SnapdragonIoT, Snapdragon Mobile,Snapdragon WiredInfrastructure and Networkingin IPQ4019, IPQ8064,IPQ8074, MDM9150,MDM9206, MDM9607,				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 877	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Ра	tch	NCIIP	'C ID
			QCA65 QCA65 QCA93 QCA93 QCA98 QCN55 SD 210 425, SE SD 675 670, SE SD 835 855, SE SDM63 SDX24,		6574, CA6584 CA8081 9379, Q 9886, Q 404, QC 2/SD 20 2/SD 20 2/SD 20 2/SD 71 0 820, SI 3/SD 85 DA660, 560, SDX 30	, CA9531, CA9980, S605, 5, SD D 636, L0 / SD D 820A, 50, SD				
				renderin						
Improper Input Validation	25-07-2019	2.1	backgru check i and als handlir to unin in Snapdr S	ound, Er s not cau s not cau s not cau s not cau ag is bein tended S odragon cagon Co cagon Co cagon Co cagon Co cagon Co cagon Mo cagon Mo cagon Wi ructure a 49150, M 607, MD 655, MSI 4, QCS60 0 205, SI	rror stat ught pro rect statung done SUI beha Auto, ompute, onnectivit onsumer dustrial obile, ired and Network ADM920 M9650, M8996A 05, SD 22 0 410/1 0 712 / S 0, SD 820 SD 845 /	us operly 1s leading aviour ity, ty, TOT, TOT, TOT, TOT, NU, 10/SD 2, SD SD 710 /), SD (SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX24, SXR1130		
			CVE ID : CVE-2019-2241		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1562
			CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1563
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1564
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130		
			CVE ID : CVE-2019-2254		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1565
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_6- 130819/1566
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 881	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2273		
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Noice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, DCA6574AU, QCA6174A, DCA6574AU, QCA6174A, DCA6574AU, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1567
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019-	0-QUA-SD_6- 130819/1568
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCII	PC ID
			Snapdr MSM89 QCS605 205, SD SD 435 636, SD SD 710 820A, S 850, SD SDM66	agon Mc agon Vo 996AU, Q 5, SD 21(0 425, SE , SD 450 0 665, SE / SD 67 SD 835, SE 0 855, SE 0, SDX24 : CVE-2	ice & M (CS405, 0/SD 21 0 427, SI , SD 625 0 675, SI 0, SD 73 SD 845 / 0A660, S 4	code- auror secur bullet	ity-			
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	CVE ID : CVE-2019-2277 Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016				w.cod ra.org rity- bullet	a- ity-	0-QUA 130819	-
Improper Restriction of	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently				https: w.qua m.cor		0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 883	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2281	mpany/pro duct- security/b ulletins	
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_6- 130819/1571
CV Scoring Sc					

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	PC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	inform firmwa checkin structu a kerne Auto, S Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr SD 427 439 / S SD 632 675, SI SD 730 835, SI SD 8CX SDM63 Snapdr	el driver napdrag ragon Co ragon Co ragon Mo ragon Mo ragon Wo 209W, M 5, Qualco 209W, M 5, Qualco 200W, M 5, Qualco 200	sclosure o insuffi embedd can be se in Snap gon Com onnectiv nsumer dustrial obile, nice & M earables SM8996 omm 21 D 205, S SD 450, S SD 450, S SD 450, S SD 710 / SD 820 SD 850, S 0, SD M4 S 50, SD 665 S SD 710 / S SD 820 S S SD 820 S	cient ed ent from dragon pute, ity, IOT, IOT, USIC, SD 625, 5, SD SD 625, 5, SD SD 625, 5, SD SD 670, OA, SD SD 855, 39, _2016,	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
Out-of- bounds Write	22-07-2019	7.5	receive lead to issue ir Snapdr Compu Consur Industr Mobile Music, in MDM MDM9	ber valid ed from f an out o ragon Au ragon Au rer IOT, rial IOT, , Snapdra A9150, M 607, MD 650, MS 996AU, (firmwar of bound Iriver. ir Ito, Snap dragon Snapdr Snapdra agon We ADM920 M9640, M8909V	write odragon agon oice & arables 06,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

25-0/-2019 46	
Use After25-07-20194.6freeing IFE resources due to lack of length check of in port resource. in Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearableshttps://ww w.codeauro ra.org/secu rity- 0-QUA	
QCS605, SD 425, SD 427, SD july-2019- 430, SD 435, SD 450, SD 625, code- SD 636, SD 675, SD 712 / SD aurora- 710 / SD 670, SD 730, SD 845 / security- SD 850, SD 855, SDM630, bulletin CVE ID : CVE-2019-2293 Image: CVE 1D - CVE - 2019 - 2293	A-SD_6- 9/1574
10r = 125.07.2019 46 consumer licentines $19/07/01/$	A-SD_6- 9/1575
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	D	escriptic	on & CVE	ID	Pa	tch	NCIIP	C ID
			MDM92 MDM96 MSM89 QCA657 QCA937 SD 210 425, SD SD 450 636, SD SD 670 820A, S 850, SD SDX24	IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299 Out of bound access when reason code is extracted from						
Out-of- bounds Read	25-07-2019	7.5	Out of b reason frame d the frar Snapdr Consum Consum Industr Mobile, Music ii MDM92 MDM96 MSM89 QCA657 QCA937 425, SD SD 450 665, SD SD 670 820A, S 850, SD SDM66	oound a code is lata with ne lengt agon Au ner Elec tivity, S ner IOT, ial IOT, Snapdr 106, MD 206, SI 206, SI 30675, SI 30835, SI 0, SDX2	ccess wl extracte hout val th in ito, Snap tronics napdrag Snapdr Snapdra Snapdra Snapdra (Snapdra (Snapdra Snapdra (Snapdra (Snapdra (SD 845 / SD 845 /	hen ed from idating odragon agon agon oice & 4A, 7, 5605, SD D 435, 6, SD SD 710 / 0, SD 5D 710 / 0, SD 4 SD 710 /	w.cod ra.org rity- bullet	in/20 7/01/ 019- a- ity-	0-QUA- 130819	—
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 887	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pat	tch	NCIIP	CID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	while h to out o in Snapdr Snapdr Snapdr Snapdr Snapdr Mobile Music, in MDM MDM90 MSM89 QCS409 215, SI SD 425 435, SI SD 425 435, SI SD 615 632, SI SD 712 730, SI SD 845 SDA66 SDM66	Der castin nandling of bound odragon ragon Co ragon Co ragon Io ragon Io ragon Io ragon Io ragon Io ragon Io ragon Io ragon Io ragon Io ragon V ragon Io ragon Io rag	the buff I read in Auto, nnectivi nsumer dustrial Γ, Snapd agon Vo gon We 4DM920 M9650, SM8996 D5, Qualo D5, Qualo D5, Qualo D5, Qualo D5, Qualo D5, Qualo D5, Qualo D5, Qualo D5, Qualo D5, Qualo D665, SI 0 429, S 415, SD D665, SI 0 / SD 6 D 820A, S 0, SD 85 39, SDM 0	er leads display ty, IOT, IOT, ragon ice & arables 6, AU, comm D 205, 5, SD 450, 625, SD D 450, 625, SD D 675, 70, SD SD 835, 5, 630,	-	in/20 7/01/ 019- a- ity-	0-QUA- 130819	
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405,				w.cod	7/01/ 019- a- ity-	0-QUA- 130819	
CV Scoring So	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_6- 130819/1579
Improper Restriction of Operations within the Bounds of	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/	0-QUA-SD_6- 130819/1580
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Bounds of a MemoryMobile, Snapdragon Voice & Music, Snapdragon Wiredduct- security/bBufferInfrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SDulletins	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd_710_firmwaresector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Consumer Electronics Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD	-			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24	code- aurora- security-	
Improper Restriction of Operations within the Bounds of a Memory Buffer25-07-20194.6Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer Electronics Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SDoutput output output output duct security/boutput output output output consumer 2000 consumer 2000 				CVE ID : CVE-2019-2312		
SD 450, SD 625, SD 632, SD	Improper Restriction of Operations within the Bounds of a Memory		4.6	emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD	w.qualcom m.com/co mpany/pro duct- security/b	0-QUA-SD_7- 130819/1581

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				890						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			636, SD 712 / SD 710 / SD 67 SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660 SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2235		
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networkin in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomn 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 67 SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236	g https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/1582
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error cas If keypad gpio deactivation fails leads to silent failure	https://ww w.qualcom m.com/co mpany/pro	0-QUA-SD_7- 130819/1583
CV Scoring So (CVSS)	cale 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	tch	NCIIF	PC ID
			scenario and su gets executed e Snapdragon Au Compute, Snap Consumer Elec Connectivity, S Consumer IOT, Industrial IOT, Mobile in MDM MDM9607, MD MDM9655, QC 210/SD 212/S 410/12, SD 67 5XR1130	everytime in ito, Snapdrago odragon stronics napdragon Snapdragon 19206, M9650, S605, SD D 205, SD D 205, SD 5, SD 712 / SI SD 730, SD 8C	on ulletin			
Out-of- bounds Read	25-07-2019	4.6	CVE ID : CVE-2019-2237 Lack of check of data type can lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2238		vill to https: w.qua m.con mpan duct- securi ulletin	n/co y/pro ity/b	0-QUA- 130819	_
Improper Input Validation	25-07-2019	2.1	Sanity checks a layout which ca Corruption or o Denial of Servi	w.qua m.con		0-QUA- 130819		
CV Scoring So (CVSS)	cale 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		Pa	tch	NCIIP	CID
			Snapdragon Au Compute, Snap Connectivity, S Consumer Elect Connectivity, S Consumer IOT, Industrial IOT, Mobile, Snapdra Music, Snapdra Infrastructure in MDM9150, M MDM9607, MD MDM9640, MD MDM9640, MD MDM9655, MS QCS404, QCS60 215, SD 210/SI SD 410/12, SD 430, SD 435, SI SD 450, SD 615 625, SD 632, SI 650/52, SD 632, SI 650/52, SD 675 710 / SD 670, S SD 820A, SD 83 850, SD 8CX, SI SDM439, SDM6 SDX20, SDX24, Snapdragon_Hi SXR1130 CVE ID : CVE-2	dragon napdragon napdragon tronics napdragon Snapdrag Snapdrag ragon Voice and Netwo MDM9206 M9650, M9650, M8996AU 05, Qualco D 212/SD 425, SD 4 0 439 / SD 5/16/SD 4 0 636, SD 5, SD 712 , SD 730, SD 85, SD 845 DA660, 530, SDM6	n n gon on æ & d orking , mm 205, 27, SD 0 429, 15, SD 0 429, 15, SD 0 820, 5 / SD 0 820, 5 / SD	duct- secur ulletin	• •		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon			w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring Sc	cale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Ра	tch	NCIII	PC ID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240				
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	—
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130		
			CVE ID : CVE-2019-2241		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/1588
Improper Input	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in	https://ww w.qualcom m.com/co	0-QUA-SD_7- 130819/1589
Validation			Snapdragon Auto, Snapdragon	mpany/pro	
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SE 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	duct- security/b ulletins	
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_7- 130819/1590
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 896	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254			
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1591	
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information	https://ww w.qualcom m.com/co mpany/pro	0-QUA-SD_7- 130819/1592	
CV Scoring So			2-3 3-4 4-5 5-6	6-7 7-8		

Weakness	Publish Date	CVSS	Description & CVE ID			Pat	tch	NCIIP	CID	
			disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261				duct- securi ulletin	51		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD			w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
			Quint	51, QUA	, JUO, JL	,		i i	4	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263			
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1594	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670,	bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1595	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130			
			CVE ID : CVE-2019-2269			
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1596	
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_7- 130819/1597	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2273		
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1598
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_7- 130819/1599
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	C ID
			SD 710 820A, 9 850, SI	0 665, SI / SD 67 SD 835, S 0 855, SI 00, SDX2	70, SD 73 SD 845 / DA660, S	30, SD				
			CVE ID	: CVE-2	2019-22	77				
Improper Authentica tion	25-07-2019	7.2	ignored bypass verifica Auto, S IOT, Sn MDM9 SD 427 450, SI SD 710 850, SI	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 CVE ID : CVE-2019-2278 Shared memory gets updated with invalid data and may lead to access beyond the allocated				//ww eauro g/secu in/20 7/01/ 019- a- ity- in	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	with in to acce memor Snapdr Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 MSM89 QCS409 215, SI SD 425 450, SI SD 665 710 / S SD 820	Shared memory gets updated				//ww eauro s/secu in/20 5/03/ 2019- a- ity- in	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	C ID
			-	agon_H	igh_Med 2019-22					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	image of memori cause of code. in Snapdn Snapdn Snapdn Snapdn QCS40 665, SI SD 670 835, SI SD 8CX SDM66	onnectiv onsumer dustrial obile, oice & M 05, SD 63 0, SD 63 0, SD 820 50 850, S 0, SD 820 4, SXR1	to ntly erified ompute, ity, IOT, IOT, USIC in 36, SD SD 710 /), SD SD 855, 530, 130	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819		
NULL Pointer Dereferenc e	25-07-2019	7.8	CVE ID : CVE-2019-2281 Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665,					//ww ilcom n/co y/pro ity/b ns	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2343	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/1604
Concurrent Execution using Shared Resource with Improper	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019-	O-QUA-SD_7- 130819/1605
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Synchroniz ation ('Race Condition')			in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2345	code- aurora- security- bulletin		
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/1606	
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1607	
CV Scoring So	cale 0-1	1-2	2-3 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, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1608
Improper Restriction of Operations within the	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20	0-QUA-SD_7- 130819/1609
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 906	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Des	cription	& CVE	ID	Pat	tch	NCIIF	PC ID
Bounds of a Memory Buffer			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292 Pointer dereference while				19/06 june-2 code- aurora securi bullet	2019- a- ty-		
Use After Free	25-07-2019	4.6	CVE ID : CVE-2019-2292 Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 /				https: w.cod ra.org rity- bullet 19/07 july-2 code- aurora securi bullet	eauro /secu in/20 7/01/ 019- a- ty-	0-QUA- 130819	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,			https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins		0-QUA- 130819		
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1612
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670 SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 CVE ID : CVE-2019-2301	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1613
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SI 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 , SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1614
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2305		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1615
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_7- 130819/1616
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307			
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1617	
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur	https://ww w.codeauro ra.org/secu	0-QUA-SD_7- 130819/1618	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 911	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	[Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			since d exceed Snapdr Consur Consur Industr Mobile Music i MDM9 MSM89 QCA65 QCA93 205, SI SD 712 820A, S SDM66		a- ity-					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID When I comma potenti to lack data bu Snapdr Consur Consur Industr Mobile Music i MDM9 QCA61 QCA93 QCS60 205, SI SD 435 625, SI SD 712 730, SI SD 845	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819				
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID			Ра	tch	NCIIP	PC ID	
			SDM63	0, SDM6	60, SDX	24				
l			CVE ID	: CVE-2	019-23	12				
sd_712_firm	iware									
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	emulat sector s TA roll Snapdr Compu Connec Consur Industr Mobile, Music, S Infrastr in MDM MDM90 MSM89 QCS60 410/12 430, SE SD 450 636, SE SD 820 845 / S SDM43 Snapdr SXR113 CVE ID	ragon Au te, Snap ctivity, Si ner Elec ctivity, Si ner IOT, rial IOT, , Snapdr Snapdra ructure a (19206, M 650, MD 996AU, Q 5, Qualco 2, SD 425 0, SD 45 0, SD 4	B is used imption otection ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra agon Vo gon Wir and Netw ADM9605 M9655, QCS404, DM9655, QCS404, DM9655, QCS404, SD 632 SD 710 / A, SD 632 SD 710 / A, SD 83 SD 8CX, S SD 8CX, S SO 8CX, S SO 8CX, S SO 8CX, S SO 8CX, S	l due to s in the logic. in odragon gon agon ice & red working 07, 5, SD 7, SD 5, SD 7, SD 5D 429, 2, SD SD 670, 35, SD SD 670, 35, SD SD 660, 1660, _2016, 35	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,			w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819		
			Snapdr	agon Co	nsumer	IOT,				
CV Scoring S	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2236		
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/1622
CV Scoring So (CVSS)	cale 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	n & CVE	ID	Ра	tch	NCIIP	C ID
Out-of- bounds Read	25-07-2019	4.6	still eva buffer u Snapdra Comput Consum Connect Consum Industri MDM96 210/SD 410/12 710 / SI SXR113	subsequ ion pote e and th luate to nderflo agon Au ce, Snap ner Elec tivity, Sp ner IOT, ial IOT, ial IOT, 55, QCS 212/SI , SD 675 0 0	ent loo entially e condi true lea w. in to, Snap dragon tronics napdrag Snapdra 9206, M9650, S605, SE 5, SD 71 D 730, S	p- go tion will ading to odragon gon agon agon 2 / SD SD 8CX,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
Improper Input Validation	25-07-2019	2.1	layout v Corrupt Denial o Snapdra Comput Connect Consum Industri Mobile, Music, S Infrastr in MDM MDM96 MDM96 QCS404	Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired		w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	_	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3	3-4 915	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descri	ption & CVE	ID	Ра	tch	NCIIP	CID
			430, SD 435 SD 450, SD 625, SD 632 650/52, SD 710 / SD 67 SD 820A, SI 850, SD 8CX SDM439, SI SDX20, SDX Snapdragon SXR1130 CVE ID : CV	615/16/SD 615/16/SD 675, SD 71 0, SD 730, S 0 835, SD 84 5, SDA660, 0M630, SDN 24, _High_Med	415, SD D 2 / SD SD 820, 45 / SD 4660, _2016,				
N/A	25-07-2019	2.1	While sendi surface com Error handl checked res unpredictal Snapdragor Compute, Sr Connectivity Consumer E Consumer I Industrial IC IoT, Snapdr Snapdragor Snapdragor Snapdragor Infrastructu in IPQ4019, IPQ8074, M MDM9206, MDM9640, MSM8996A QCA6564, Q QCA6574AU QCA6584AU QCA6584AU QCA9377, Q QCA9880, Q SD 210/SD 425, SD 600	tent to the s ing is not p ults in an ole behavior Auto, Snap napdragon y, Snapdrag OT, Snapdrag	screen, roperly ur in odragon gon agon e, usic, working 4A, 4A, 5, CA9531, CA9531, CA9980, 5605, 5, SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring S	cale 0-1	1-2	2-3 3-4		5-6	6-7	7-8	8-9	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130	,	
			CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networkin in MDM9150, MDM9206, MDM9607, MDM9206, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2241	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/1626
Improper Restriction of Operations within the	22-07-2019	2.1	Possible buffer overflow at th end of iterating loop while getting the version info and lead to information disclosure in Snapdragon Auto,	w.qualcom m.com/co	0-QUA-SD_7- 130819/1627
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 917	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
Bounds of a Memory Buffer			Snapdr Snapdr Snapdr Mobile Music, in MDM MSM89 210/SI SD 427 439 / S 615/16 632, SI SD 712 730, SI SD 845 SDA66 SDM66	ragon Co ragon Co ragon Ind ragon Io , Snapdra A9206, M 650, MSI 996AU, Q 0 212/SI 7, SD 430 0 212/SI 7, SD 430 50 429, S 6/SD 415 0 636, SE 6/SD 415 0 636, SE 6/SD 71 0 820, SE 6/SD 85 0, SDM4 50 0 : CVE-2	nsumer dustrial F, Snapd agon Vo gon We (DM960 M8909V (CS605, D 205, SI (CS605, SI (CS60	IOT, iragon ice & arables 07, V, SD D 425, 5, SD D 425, 5, SD 5, SD 5, SD 0 675, 70, SD SD 835, 55, 630,	secur ulletin	• •		
Improper Input Validation	25-07-2019	7.5	while p corrup Snapdr Connec Consur Industr IoT, Sn Snapdr MDM9 MDM9 MDM9 MSM89 QCS409 215, SI SD 425 435, SI SD 600 625, SI SD 675	ted cominagon Au ctivity, Si ner IOT, rial IOT, apdrago ragon Vo ragon We 150, MD 607, MD 607, MD 5, QCS60 0 210/SI 5, SD 427 0 439 / S	n ogg fil ment blo ito, Snap napdrag Snapdra Snapdra Snapdra n Mobil ice & Mi earables M9206, M9650, SM8996 05, Qualo 05, Qualo 05, Qualo 05, Qualo 0212/SI 05, Qualo 0212/SI 0429, SI /16/SD 0636, SI / SD 71	le with a ock. in odragon agon e, usic, s in 5AU, comm D 205, 0, SD 5D 450, 415, SD D 665, 0 / SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 918	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/1629
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/	0-QUA-SD_7- 130819/1630
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260	june-2019- code- aurora- security- bulletin	
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD		O-QUA-SD_7- 130819/1631
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1632
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019-	O-QUA-SD_7- 130819/1633
CV Scoring So (CVSS)	cale 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		Pa	tch	NCIIP	CID
			in MDM9607, M MSM8909W, Q0 SD 425, SD 427, 435, SD 439 / S SD 625, SD 632, 712 / SD 710 / 820A, SD 835, S 850, SDM439, S SDM660, SDX24 CVE ID : CVE-20	code- auror secur bullet	ity-				
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer processing the l process action f improper buffer validation in Sn Snapdragon Cor Snapdragon Cor Snapdragon Ind Snapdragon Mo Snapdragon Mo Snapdragon Voi MDM9150, MDI MSM8996AU, Q QCS605, SD 625 665, SD 712 / S SD 730, SD 820, 835, SD 845 / S SDA660, SDM63 SDX20, SDX24, S	high level li Frame due t r length apdragon A mpute, nsumer IOT lustrial IOT bile, ice & Music M9650, CS405, 5, SD 636, S D 710 / SD , SD 820A, S D 850, SD 8 30, SDM660 SXR1130	im to Auto, Γ, Γ, c in 5D 670, SD 355,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,			w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4	4-5 5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20		
			CVE ID : CVE-2019-2272		
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/1636
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-	O-QUA-SD_7- 130819/1637
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276	security- bulletin	
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1638
Improper Authentica tion	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	O-QUA-SD_7- 130819/1639
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publi	sh Date	CVSS	•					tch	NCIIP	CID
				850, SI	DM660			bullet	in		
				CVE ID) : CVE-2	2019-22	278				
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07	7-2019	7.5	with in to acce memor Snapdr Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 MDM9 MSM89 QCS40 215, SI SD 425 450, SI SD 665 710 / S SD 820 850, SI SDM63 SDX24 Snapdr	nd the al apdrago onnectiv dustrial obile, oice & M earables M9607, M8909V QCA657 0, Qual- 0, SD 42 0, SD 42 0, SD 712 5, SD 712 5, SD 84	nay lead llocated n Auto, ity, IOT, IOT, usic, s in V, 4AU, comm D 205, 29, SD D 636, 2 / SD SD 820, 45 / SD SDM439, 320,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07	7-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130		
			CVE ID : CVE-2019-2281		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_7- 130819/1642
			CVE ID : CVE-2019-2334 Out of bound read and		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_7- 130819/1643
CV Scoring So (CVSS)	cale 0-1	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	°C ID
			Snapdragon Mo Snapdragon Voi Snapdragon Voi MSM8909W, MS QCS605, Qualco 210/SD 212/SD SD 427, SD 430, 439 / SD 429, SI SD 632, SD 636, 675, SD 712 / SI SD 730, SD 820, 835, SD 845 / SI SD 8CX, SDA660 SDM630, SDM60 Snapdragon_Hig SXR1130 CVE ID : CVE-20					
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition of DMA buffer in jp Snapdragon Aut Connectivity, Sm Consumer IOT, S Industrial IOT, S Mobile, Snapdra in MSM8909W, QCS605, SD 425 430, SD 435, SD SD 636, SD 712 670, SD 820, SD SD 845 / SD 850 SDM660, SDX20 CVE ID : CVE-20	https:/ w.code ra.org/ rity- bulleti 19/07 july-20 code- aurora securi bulleti	eauro /secu n/20 /01/ 019- a- ty-	0-QUA- 130819	_	
Improper Validation of Array Index	25-07-2019	7.2	Firmware is get of overwriting r scan command i host because of validation. in Sn Compute, Snapo Consumer IOT, S Industrial IOT, S	https:/ w.qual m.com mpany duct- securi ulletin	lcom 1/co 7/pro ty/b	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1646
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead	https://ww w.codeauro	0-QUA-SD_7- 130819/1647
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 928	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	5 Description & CVE ID camera driver to access				Pa	tch	NCIIP	CID
			destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290 Out of bound access can occur due to buffer copy without				rity-	019- a- ity-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur		w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819			
Use After	25-07-2019	4.6	CVE ID : CVE-2019-2292Pointer dereference while				https:	//ww	0-QUA-	SD_7-
CV Scoring Sc (CVSS)	ale 0-1	1-2	2-3	3-4 929	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Ра	tch	NCIIP	CID
Free			freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2293 Protection is missing while				ra.org rity- bullet	a- ity-	130819	/1649
Use After Free	25-07-2019	4.6			w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819			
Integer Overflow or Wraparou	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in				https://ww w.codeauro ra.org/secu rity-		0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 930	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description	on & CVE I	ID	Pat	tch	NCIIP	C ID
nd			Snapdragon Au Consumer Elec Connectivity, S Consumer IOT Industrial IOT, Mobile, Snapdra Infrastructure in IPQ4019, IP IPQ8074, MDM MDM9206, ME MDM9640, ME MDM9640, ME MDM9640, ME MDM9640, ME MSM8996AU, Q QCA6574AU, Q QCA6574AU, Q QCA6574AU, Q QCA6574AU, Q QCA6574AU, Q QCA6574AU, Q SD 210/SD 212 425, SD 427, SI SD 450, SD 600 636, SD 675, SI SD 670, SD 730 820A, SD 835, SDX24 CVE ID : CVE-2	bullet 19/07 july-2 code- auror securi bullet	2019- a- ity-				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of o read if id recei not in range of Snapdragon Au Compute, Snap Consumer IOT Industrial IOT, Mobile, Snapdu Wearables, Sna Infrastructure in IPQ4019, IP MSM8909W, M QCA9980, QCS 215, SD 425, SI SD 450, SD 625 636, SD 712 / 2 SD 820A, SD 84	w.cod	7/01/ 019- a- ity-	0-QUA- 130819			
			00 02011, 00 0	10 / 00 0	130, 30		I		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SDM439, SDM660, SDX24		
			CVE ID : CVE-2019-2301		
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_7- 130819/1653
			CVE ID : CVE-2019-2305		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_7- 130819/1654
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_7- 130819/1655
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the	https://ww w.codeauro ra.org/secu	0-QUA-SD_7- 130819/1656
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 933	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308 While storing calibrated data from firmware in cache, An					a- ity-		
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data		w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 934	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20		
			CVE ID : CVE-2019-2309		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow de to lack of input validation of data buffer received in Snapdragon Auto, Snapdrage Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS40 QCS605, SD 210/SD 212/SI 205, SD 425, SD 427, SD 43 SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 67 SD 712 / SD 710 / SD 670, S 730, SD 820, SD 820A, SD 8 SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	of https://ww https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin 5, SD	0-QUA-SD_7- 130819/1658
sd_820_firm	iware				·
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs whe emulated RPMB is used due sector size assumptions in to TA rollback protection logic Snapdragon Auto, Snapdrago Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	e to the c. in https://ww gon w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1659
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5 -	-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Ра	tch	NCIIP	CID
			in MDM MDM90 MSM89 QCS609 410/12 430, SE SD 450 636, SE SD 820 845 / S SDM43 Snapdr SXR113	1DM960 M9655, (CS404, omm 21 5, SD 42 0 439 / S , SD 632 5D 710 / A, SD 83 5D 8CX, S 0 8CX, S 0 8CX, S 0 8CX, S 0 8CX, S 0 8CX, S 0 8CX, S	5, SD 7, SD 5D 429, 2, SD 5D 670, 35, SD 5DA660, 1660, _2016,					
NULL Pointer Dereferenc e	25-07-2019	2.1	CVE ID : CVE-2019-2235 Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD				w.qua m.cor mpan duct- secur ulletin	n/co y/pro ity/b	0-QUA- 130819	
			SDM43	9, SDM6	DA660, 530, SDN	1660,				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2236		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1661
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an	https://ww w.qualcom m.com/co mpany/pro	0-QUA-SD_8- 130819/1662
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

		· ·	lictable b	ehavior	ır in	duct-			
		Compu Connect Consur Consur Industr IoT, Sn Snapdr Snapdr Infrastr in IPQ4 IPQ807 MDM92 MDM92 MDM92 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 QCA65 SD 210 425, SI SD 675 SD 210 425, SI SD 675 SD 835 SD 835 SDX24,	ragon Au ite, Snape ctivity, Sn ner Elect ctivity, Sn ner IOT, rial IOT, S apdrago ragon Vo ragon Wi ructure a 4019, IPC 74, MDM 206, MD 640, MD 640, MD 640, MD 640, MD 640, MD 640, MD 640, MD 640, MD 640, MD 602, QC 80, QCA 602, QC 80, QC 80, SD 712 0 600, SD 600, SD 60, SD 712 0 730, SD	tto, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra Snapdra n Mobile ice & Mu ired and Netw 28064, 9150, M9607, M9650, 2064, 0404, QCS 20574, CA65844 CA65844 CA65844 CA65844 CA6584 CA65	dragon on agon agon e, isic, working AA, A, CA9531, CA9531, CA9980, 5605, 5, SD 0 636, 0 / SD 0 820A, 0, SD 2 0,	securi			
Improper Input 25-07-20 Validation	19 2.1	backgro check i and als handlir to unin in Snap Snapdr	renderin ound, Er s not cau so incorre ng is beir itended S odragon Co ragon Co	ror statu ight pro ect statu ng done SUI beha Auto, mpute,	us perly Is leading Iviour	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
1		2-3	3-4	4-5	-	6-7			9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
			Snapdr Snapdr Snapdr Snapdr Infrast in MDM MDM9 QCS40 212/SI 636, SI SD 670 820A, S 850, SI SDM63	Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2241						
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possibl end of getting lead to in Snapdr Snapdr Snapdr Snapdr Mobile Music, in MDM MDM9 MSM89 210/SI SD 427 439 / S 615/10 632, SI SD 712 730, SI SD 845	CVE ID : CVE-2019-2241 Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835,		w.qua m.cor mpan duct- secur ulletin	n/co y/pro ity/b ns	0-QUA- 130819	/1664	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 939	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1665
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1666
CV Scoring So (CVSS)	cale 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	Ра	tch	NCIIP	PC ID
			MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2254							
N/A	22-07-2019	4.9	Unauth subsys non see can lea disclos Snapdr	tem to H cure sub d to info ure in Si ragon Co ragon Co ragon Co ragon Mo ragon Mo ragon W	access fr ILOS or a system ormation napdrag ompute, onnective onsumer dustrial obile, oice & M ired and Net DM9150 M9607, M8996A 605, Qua D 212/S 7, SD 430 SD 429, S 2, SD 636 5, SD 71	om GPU other memory on Auto, ity, IOT, IOT, usic, working , U, alcomm D 205, 0, SD SD 450, 5, SD 2 / SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1668
			Possible buffer overflow while	https://ww	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	w.codeauro ra.org/secu rity-	0-QUA-SD_8- 130819/1669
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670 SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269	security- bulletin	
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730 SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1670
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,		0-QUA-SD_8- 130819/1671
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 943	6-7 7-8	8-9 9-10

Weakness	Publish [Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
				Snapdr Snapdr MDM9 MDM9 MSM89 QCS40 215, SI SD 425 450, SI SD 665 710 / S SD 820 850, SI SDM63 SDX24 Snapdr CVE ID	auror securi bullet	ity-					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-20	019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
NULL Pointer Dereferenc e	25-07-20	019	7.8	happer with w Snapdr Compu	ointer de 1 when p rong blo ragon Au 1te, Snap ner IOT,	olaying t ock grou ito, Snap dragon	he clip p id in odragon	https: w.qua m.con mpan duct- secur	n/co y/pro	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			Industr IoT, Sn Snapdr Snapdr MDM9 MDM9 MSM89 QCS40 215, SI SD 425 435, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63 Snapdr CVE ID	ulletin	ns					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670,				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 945	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2343		
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2345	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1675
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660	security/b ulletins	0-QUA-SD_8- 130819/1676
CV Scoring So (CVSS)	cale 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	Descriptio	otion & CVE ID			tch	NCIIF	PC ID
			CVE ID : CVE-2019-2346							
Out-of- bounds Write	22-07-2019	7.5	issue in Snapdn Comput Consur Industr Mobile Music, in MDM MDM9 MDM9 MDM9 MSM89 QCS40 215, SI SD 425 435, SI SD 625 665, SI SD 670 820A, S 850, SI SDM63 SDX24	lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287 Multiple open and close from				c//ww leauro g/secu in/20 6/03/ 2019- a- ity- in	0-QUA- 130819	
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290		
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1679
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1680
CV Scoring So	cale 0-1	1-2	2-3 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 IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299		
			Out of bound access when reason code is extracted from frame data without validating the frame length in		
Out-of- bounds Read	25-07-2019	7.5	Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1681

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				949						

Weakness	Publish Date	CVSS	Description & CVE ID			Pa	tch	NCIIP	CID	
			CVE ID	: CVE-2	019-23	05				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306					//ww leauro g/secu in/20 7/01/ 019- a- ity- in	0-QUA- 130819	
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU,				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIF	PC ID
			QCA93 QCS60! 205, SE SD 435 625, SE SD 712 730, SE SD 845 SDM63 SDX24	74A, QCA 77, QCA 5, SD 21(0 425, SD 6, SD 450 0 636, SD 7 SD 71 0 820, SD 6 / SD 85 60, SDM6 9 : CVE-2	9379, Q 0/SD 21 0 427, SI 0, SD 600 0 665, SI 0 / SD 6 0 820A, S 0, SD 85 660, SDX					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2307 When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
sd_835_firm	iware									
Improper Restriction of	25-07-2019	4.6		when l due to s in the	https: w.qua m.cor		0-QUA- 130819			
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 951	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2235		
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1686
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2236		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1687
CV Scoring S (CVSS)	cale 0-1	1-2	650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, 2-3 3-4 4-5 5-6 953	6-7 7-8	8-9 9-10

N/A25-07-20192.1SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130Https://ww w.qualcom connectivity.Snapdragon Connectivity.Snapdragon Connectivity.Snapdragon Connectivity.Snapdragon Connectivity.Snapdragon Industrial IOT, Snapdragon MDM940, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MDM9640, MDM9650, MDM9640, MDM9650, MDM9640, QCA65744, QCA65744U, QCA6574, QCA65744U, QCA6584, QCA65744U, QCA6584, QCA57540U, QCA6584, QCA57540U, QCA6584, QCA57540U, QCA6584, QCA57540U, QCA6584, QCA57540U, QCA6584, QCA57540U, QCA6584, QCA57540U, QCA6584, QCA57540U, QCA9880, QCA9980, QCN5502, QCS404, QC3605, SD 210/SD 212/SD 210/SD 210/SD 212/SD 210/SD 20/SD 20/	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
 N/A 25-07-2019 25-07-2019 Auto, Sapdragon Auto, Snapdragon Consumer Electronics NAP 25-07-2019 Auto, Sapdragon Mobile, Snapdragon Mobile, Consumer IDT, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon NAP 404019, IPQ8064, Ini PQ4019, IPQ8064, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6574, QCA6574AU, QCA6574, QCA6574AU, QCA6574, QCA6574AU, QCA6584, QCA6574AU, QCA6584, QCA6574AU, QCA6584, QCA6574AU, QCA6584, QCA6574AU, QCA6584, QCA6574AU, QCA6584, QCA6574AU, QCA6505, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 670, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 82				SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239		
	N/A	25-07-2019	2.1	surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial VT, Snapdragon Industrial NT, Snapdragon Infastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD	w.qualcom m.com/co mpany/pro duct- security/b	÷

CV Scoring Scale (CVSS) 0-1

1-2

2-3

3-4

954

5-6

6-7

8-9

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIF	PC ID
			CVE ID	: CVE-2	019-22	40				
Improper Input Validation	25-07-2019	2.1	backgr check i and als handlin to unin in Snapdn Sn	49150, N 607, MD 655, MS 4, QCS6(0 205, SI 0 675, SI 0 675, SI 50 835, SI 80, SDM6	ror stat ught pro ect statu- ng done SUI beha Auto, mpute, mectivit msumer mectivit onsumer dustrial obile, ired and Netw /DM920 M9650, M8996A 05, SD 21 0 410/1 0 712 / S 0, SD 820 SD 845 / 0 8CX, SI 560, SDX	us perly is leading aviour ity, y, IOT, IOT, IOT, ior, ior, ior, SD 2, SD 5D 710 / 0, SD 2 SD 2A660, 24,	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	_
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 955	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	e CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1691
Informatio	25-07-2019	7.5	Position determination	https://ww	O-QUA-SD_8-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Des	cription &)	Pa	tch	NCIIF	PC ID
n Exposure			accuracy i to wrongly informatio Auto, Snap Snapdrage Snapdrage Snapdrage Mobile, Sr Music, Sna in MDM9607 MDM9607 MDM9607 MDM9607 MDM9667 MDM9667 MDM9655 MSM8996 Qualcomm 212/SD 20 SD 430, SI 429, SD 45 SD 430, SI 429, SD 45 SD 650/57 SD 820, SI 845 / SD 8 SDA660, S SDA660, S SDA660, S SDA660, S SDA660, S SDA660, S	y decode on in Sna pdragon on Consu on Indus on IoT, S napdragor 150, MDM9 5, MDM9 5, MDM9 5, MSM89 5, MSM89 5, MSM89 5, MSM89 5, SD 42 0, SD 43 5, SD 42 0, SD 61 25, SD 63 2, SD 669 710 / SD 0 820A, S 850, SD 8 50M439, SDX20, on_High_	ed apdrag Comp Imer I trial IC napdr on Void n Wear M9206 615, 635M 650, 909W, 605, 0 210/ 25, SD 0 439, 15/16, 32, SD 670, S SD 835 SD 835 SD 835 SDM6 _Med_2	gon ute, OT, agon ce & rables rables 5, / SD 427, / SD 636, 075, SD 636, 075, SD 50 730, 5, SD 0 8CX, 30, 2016,	w.qua m.com duct- secur: ulletin	n/co y/pro ity/b	130819	9/1692
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,			w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
CV Scoring So (CVSS)	cale 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 & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1694
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
			SXR11	30						
			CVE ID	: CVE-2	2019-22	61				
Use After Free	25-07-2019	4.6	happer diag dr free iss Snapdr Snapdr Snapdr Snapdr Snapdr Infrast in IPQ4 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 SM89 QCA95 210/SI SD 427 450, SI 650/52 670, SI SD 845 SDX20 Snapdr	onnectiv onsumer dustrial obile, earables ired and Net Q8064, M9650, M9650, SM8996 9980, SI 0 205, S 0 205, S 0, SD 435 0 636, S 2 / SD 7	from after on Auto, ity, IOT, IOT, S, working 6AU, D 0 425, 5, SD D 10 / SD SD 835, 660, _2016	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	-	
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 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	escriptic	on & CVE	ID	Ра	tch	NCIIP	CID
			820A, SI 850, SD SDM660	M439, S	, SDM630					
			CVE ID	: CVE-2	019-22	64				
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Snapdra Snapdra Snapdra Snapdra MDM91 MSM899 QCS605	rel lim ue to on Auto, IOT, IOT, USIC in 6, SD SD 670, OA, SD SD 855, I660, 30	w.cod ra.org rity- bullet 19/00	a- ity-	0-QUA- 130819			
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD				w.cod ra.org rity- bullet 19/00	a- ity-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
					0, SDX2						
					: CVE-2						
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07	-2019	7.5	with in to acce memor Snapdr Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 MDM9 MSM89 QCS40 215, SI SD 425 450, SI SD 425 710 / S SD 820 850, SI SD 820 850, SI	nd the al apdrago innectiv insumer dustrial obile, ice & M earables M9607, M8909V QCA657 0, Qualio 0, QA657 0, Qualio 0, SD 42 0, SD 42 0, SD 712 5, SD 712 5, SD 84	hay lead located n Auto, ity, IOT, IOT, usic, s in V, 4AU, comm D 205, 29, SD D 636, 2 / SD SD 820, 45 / SD SD 820, 45 / SD SDM439, 20,	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07	-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD				w.qua m.cor mpan duct- secur ulletin	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130		
			CVE ID : CVE-2019-2281		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1701
			CVE ID : CVE-2019-2334 Out of bound read and		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1702
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description 8	& CVE ID	Pat	ch	NCIIF	PC ID
			Snapdragon Mobi Snapdragon Voice Snapdragon Wear MSM8909W, MSM QCS605, Qualcom 210/SD 212/SD 2 SD 427, SD 430, S 439 / SD 429, SD SD 632, SD 636, S 675, SD 712 / SD SD 730, SD 820, S 835, SD 845 / SD SD 8CX, SDA660, S SDM630, SDM660 Snapdragon_High SXR1130 CVE ID : CVE-201					
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition will DMA buffer in jpe Snapdragon Auto, Connectivity, Snap Consumer IOT, Sn Industrial IOT, Sn Mobile, Snapdrag in MSM8909W, M QCS605, SD 425, S 430, SD 435, SD 4 SD 636, SD 712 / 670, SD 820, SD 8 SD 845 / SD 850, S SDM660, SDX20, S CVE ID : CVE-201	https:/ w.code ra.org/ rity- bulleti 19/07 july-20 code- aurora securi bulleti	eauro /secu in/20 /01/ 019- a- ty-	0-QUA- 130819	_	
Improper Validation of Array Index	25-07-2019	7.2	Firmware is gettin of overwriting me scan command is host because of in validation. in Snap Compute, Snapdra Consumer IOT, Sn Industrial IOT, Sn	https:/ w.qual m.com mpany duct- securi ulletin	lcom 1/co 7/pro ty/b	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1705
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead	https://ww w.codeauro	0-QUA-SD_8- 130819/1706
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 964	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	CID
			camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290 Out of bound access can occur				rity- bullet	a- ity-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6					w.cod ra.org rity-	2019- a- ity-	0-QUA- 130819	
Integer	25-07-2019	4.6	CVE ID : CVE-2019-2292 An out-of-bound write can be			can be	https:	//ww	0-QUA-	SD_8-
CV Scoring Sc (CVSS)	ale 0-1	1-2	2-3	3-4 965	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparou nd			triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	130819/1708
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1709
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1710
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20	O-QUA-SD_8- 130819/1711
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 967	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA65, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307	19/07/01/ july-2019- code- aurora- security- bulletin	
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1712
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 968	6-7 7-8	8-9 9-10

			Description & CVE ID SD 845 / SD 850, SD 855,				tch	NCIIP	
			SD 845 / SD 85 SDA660, SDM4 SDM660, SDX2	39, SDM	630,				
			CVE ID : CVE-2	019-23	08				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA65, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312			w.cod ra.org rity-	019- a- ity-	0-QUA- 130819	
sd_845_firm	ware								
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon			w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Ра	tch	NCIIP	PC ID
			Mobile Music, Infrast in MDM MDM9 MSM89 QCS60 410/12 430, SI SD 450 636, SI SD 820 845 / S SDM43 Snapdr SXR113 CVE ID							
Improper Input Validation	25-07-2019	2.1	SXR1130 CVE ID : CVE-2019-2235 Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD				w.qua m.com	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2239		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6584, QCA6584AU, QCA6574, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD		0-QUA-SD_8- 130819/1716
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130		
			CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2241	security/b ulletins	0-QUA-SD_8- 130819/1717
Improper Restriction of Operations within the	erations thin the unds of femory	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto,	https://ww w.qualcom m.com/co mpany/pro	0-QUA-SD_8- 130819/1718
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	duct- security/b ulletins	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660		
Improper Input Validation	25-07-2019	7.5	CVE ID : CVE-2019-2243 Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1719

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				973						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDX20, Snapdragon_High_Med_2016, SXR1130	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1720
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code-	0-QUA-SD_8- 130819/1721
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 974	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260				auror secur bullet	ity-		
N/A	22-07-2019	4.9					w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2263	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1723
NULL Pointer Dereferenc e	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora-	0-QUA-SD_8- 130819/1724
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24	security- bulletin	
			CVE ID : CVE-2019-2264		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_8- 130819/1725
			Buffer overflow can occur in		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_8- 130819/1726
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20		
			CVE ID : CVE-2019-2272		
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1727
Out-of- bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Mobile, Snapdragon Voice & Music in	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1728
CV Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2276		
Out-of- bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_8- 130819/1729
Improper Authentica tion	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1730

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
070										

Weakness	Publish Date	CVSS	Description & CVE ID		ID	Pa	tch	NCIIP	CID	
			CVE ID) : CVE-2	2019-22	78				
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279				w.cod ra.org rity- bullet 19/06 june-2 code- auror secur bullet	a- ity-	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855,				w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

0-1	1-2

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2281		
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1733
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1734
CV Scoring So (CVSS)	cale 0-1	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	Pa	tch	NCIIF	PC ID
			SD 427, SD 430 439 / SD 429, S SD 632, SD 636 675, SD 712 / S SD 730, SD 820 835, SD 845 / S SD 8CX, SDA66 SDM630, SDM6	Vearables in ASM8996AU, comm 215, SD D 205, SD 425, D, SD 435, SD SD 450, SD 625, 6, SD 665, SD SD 710 / SD 670 D, SD 820A, SD SD 850, SD 855, 50, SDM439, 660, igh_Med_2016,	,			
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	DMA buffer in Snapdragon Au Connectivity, S Consumer IOT Industrial IOT, Mobile, Snapdu in MSM8909W QCS605, SD 42 430, SD 435, S SD 636, SD 712	uto, Snapdragon Snapdragon , Snapdragon , Snapdragon ragon Wearables 7, MSM8996AU, 25, SD 427, SD D 450, SD 625, 2 / SD 710 / SD D 820A, SD 835, 50, SDA660, 20, SDX24	https: w.cod ra.org rity-	019- a- ity-	0-QUA- 130819	_
Improper Validation of Array Index	25-07-2019	7.2	Firmware is ge of overwriting scan command host because o validation. in S Compute, Snap Consumer IOT Industrial IOT, Mobile, Snapda	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346		
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1737
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access	https://ww w.codeauro ra.org/secu	0-QUA-SD_8- 130819/1738
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 983	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	De	escriptio	n & CVE	ID	Pa	tch	NCIIP	C ID
			destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290 Out of bound access can occur					a- ity-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6					w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to				-	//ww eauro	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 984	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & C	/E ID	Pat	ch	NCIIP	CID
			lack of length check of resource. in Snapdra Consumer IOT, Snapo Industrial IOT, Snapo Mobile, Snapdragon V in MSM8909W, QCS4 QCS605, SD 425, SD 4 430, SD 435, SD 425, SD 4 430, SD 435, SD 450, SD 636, SD 675, SD 7 710 / SD 670, SD 730 SD 850, SD 855, SDM SDM660, SDX24 CVE ID : CVE-2019-2	ra.org rity- bulleti 19/07 july-20 code- aurora securi bulleti	in/20 //01/ 019- a- ty-			
Use After Free	25-07-2019	4.6	Protection is missing accessing md session macro which can lead after-free in Snapdra Snapdragon Compute Snapdragon Consum Snapdragon Industri Snapdragon Mobile, Snapdragon Woice & Snapdragon Wearabl MDM9150, MDM920 MDM9607, MDM920 MDM9650, MSM8909 QCS405, QCS605, SD 212/SD 205, SD 425, SD 430, SD 435, SD 4 625, SD 636, SD 712 SD 670, SD 820, SD 8 845 / SD 850, SD 855 SDM660, SDX20, SDX CVE ID : CVE-2019-2	https:, w.qual m.com mpany duct- securi ulletin	lcom 1/co y/pro ty/b	0-QUA- 130819		
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound wri triggered by a specia command supplied b userspace application Snapdragon Auto, Sn	https:, w.code ra.org, rity- bulleti	eauro /secu	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 985	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299	19/07/01/ july-2019- code- aurora- security- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1743

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				986						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SDM439, SDM660, SDX24		
			CVE ID : CVE-2019-2301		
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1744
			CVE ID : CVE-2019-2305 Improper casting of structure		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1745
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1746
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the	https://ww w.codeauro ra.org/secu	0-QUA-SD_8- 130819/1747
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 988	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	C	Descriptio	n & CVE	ID	Pa	tch	NCIIP	C ID
			to go th subsyst Auto, S IOT, Sn IOT, Sn Snapdr MDM97 MDM97 MDM97 QCS605 425, SE SD 439 625, SE SD 439 625, SE SD 675 670, SE SD 845 SDA660 SDM66	will allow frough to tem in Sr napdrago apdrago apdrago agon Vo agon We 150, MD 650, MD 650, MS 996AU, Q 5, Qualco 0, 427, SD 632, SD 730, SD 730, SD 730, SD 730, SD 730, SD 0, SDM4 0, SDM4 0, SDX20 : CVE-2	o the ren hapdrag on Cons n Indus n Mobil ice & Mu earables M9607, M8909W (CS405, 0 430, SI (CS405, 0 50, SI (CS405, 0 51, SI (CS405, SI	note on sumer trial e, usic, in V, 5, SD 0 435, 0, SD 0 435, 0, SD 0 665, 0 / SD SD 835, 5, 630, 4		a- ity-		
Out-of- bounds Read	25-07-2019	7.5	from fin integer since da exceed Snapdr Consum Consum Industr Mobile, Music i MDM92 MDM96 MSM89 QCA65 QCA93	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD		w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	_	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20		
			CVE ID : CVE-2019-2309		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1749
sd_850_firm	ware				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired		0-QUA-SD_8- 130819/1750
CV Scoring Sc (CVSS)	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			Informed							
			in MDM MDM90 MSM89 QCS609 410/12 430, SE SD 450 636, SE SD 820 845 / S SDM43 Snapdr SXR113	4DM960 M9655, QCS404, omm 21 5, SD 42 O 439 / S 5, SD 632 SD 710 / OA, SD 83	5, SD 7, SD SD 429, 2, SD SD 670, 35, SD SDA660, 4660, _2016,					
Improper Input 2: Validation	5-07-2019	2.1	Sanity of layout y Corrup Denial Snapdr Compu Connec Consum Consum Industr Mobile, Music, y Infrastr in MDM MDM90 MDM90 QCS404 215, SE SD 410 430, SE SD 450 625, SE	checks a which ca tion or c of Servic ragon Au te, Snap ctivity, Si ner Elec ctivity, Si ner IOT, rial IOT, , Snapdra ructure a 49150, M 607, MD 640, MD 655, MSI 4, QCS60 0 210/SI /12, SD	re missi an lead t can lead t can lead tc in ito, Snap dragon napdrag tronics napdrag Snapdra Snapdra Snapdra agon Vo gon Win and Net ADM920 M96351 M96351 M96350, M8996A D5, Qualo D 212/S 425, SD 0 439 / S 5/16/SD D 636, SI 5, SD 71	ing in co SUI to odragon gon gon agon agon oice & red working 06, M, AU, comm D 205, 427, SD SD 429, 415, SD D 2 / SD	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
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 & CVE ID	Patch	NCIIPC ID
			SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2239		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA6584, QCA9377, QCA9379, QCA9531 QCA9880, QCA9886, QCA9980 QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1752
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 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, SXR1130		
			CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2241	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1753
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1754
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 993	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Ра	tch	NCIIF	PC ID
			in MDM MDM9 210/SI SD 427 439 / S 615/16 632, SI SD 712	V, SD D 425, 5, SD 5, SD 5, SD D 675, 570, SD SD 835, 55, 1630,						
Improper Input Validation	25-07-2019	7.5	while p corrup Snapdr Connec Consur Industr IoT, Sn Snapdr MDM9 MDM9 MDM9 MSM89 QCS409 215, SI SD 425 435, SI SD 600 625, SI SD 675 670, SI SD 835 855, SI SDM63	ted com ragon Au ctivity, S ner IOT, rial IOT, apdrago ragon Vo ragon W 150, MD 607, MD 607, MD 607, MD 5, QCS60 0 210/SI 5, SD 427 0 439 / S	an ogg fi ment bl ito, Snap napdrag Snapdr Snapdr Snapdra in Mobil bice & M earables M9206, M9650, SM8990 D5, Qual D5, Qual D5, Qual D5, Qual D5, Qual D5, Qual D5, Qual D6, SD SD 429, S S 16/SD D636, S S 20, S S 20	le with a ock. in odragon agon e, usic, s in 5AU, comm D 205,), SD 5D 450, 415, SD D 665, .0 / SD D 820A, 50, SD	https w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	CID
Informatio n Exposure	25-07-2019	7.5	accuration wroth inform Auto, S Snapdu Snapdu Snapdu Mobile Music, in MDM MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9	ngly dec ation in inapdrag ragon Co ragon Io ragon Io ragon Io snapdra 49150, N 607, MD 625, MD 625, MD 640, MD 655, MS 996AU, (mm 215 0 205, SI 996AU, (mm 215 0 205, SI 9640, ND 625, SI 976AU, (mm 215 0 205, SI 0, SD 435 0, SD 435 0, SD 435 0, SD 820 50 710 / 0, SD 820 50 850, S 0, SDM4 50, SDX2 ragon_Hi	be degra oded Snapdra gon Com onsumer dustrial T, Snapd agon Vo gon We 4DM920 M9615, M9635N M9650, M9635N M9635N M9635, SD 210 O 425, SI 5, SD 210 O 425, SI 5, SD 439 O 615/10 O 632, SI 665, SD SD 670, O A, SD 83 SD 855, S 39, SDM 0, igh_Med	ded due agon pute, IOT, IOT, Iragon bice & arables 06, M, V, V, V, D/SD D 427, 0 / SD 0 427, 0 / SD 6/SD 0 636, 675, SD 675, SD 50 8CX, I630, _2016,	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206,				w.cod ra.org rity- bullet	a-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260	bulletin	
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660,	https://ww w.qualcom m.com/co	0-QUA-SD_8- 130819/1758
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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		
			CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1759
			CVE ID : CVE-2019-2263 Null pointer dereference		
NULL Pointer Dereferenc e	22-07-2019	4.6	occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SD_8- 130819/1760
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1761
			SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1762
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Out-of- bounds Read25-07-20197.8636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272https://ww wqualcom m.com/co mgany/pro duct-size SD 810, SD 435, SD 439 / SD 212/SD 205, SD 2425, SD 2427, SD 430, SD 435, SD 439 / SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 655, SD 712 / SD 710 / SD 665, SD 712 / SD 710 / SD 665, SD 675, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 6CX, SD M439, Snapdragon, High_Med_2016, SXR1130 CVE ID : CVE-2019-2273https://ww wcodeauro ra.org/security- builetin/20 19/07/11 / july-2019- code- aurora- security- builetin/20 19/07/11 / july-2019- code- aurora- security- builetin/20 19/07/11 / july-2019- code- aurora- security- builetinhttps://ww wcodeauro ra.org/security- builetin/20 19/07/11 / july-2019- code- aurora- security- builetinhttps://ww wcodeauro ra.org/security- builetin/20 19/07/11 / july-2019- code- aurora- security- builetinhttps://ww wcodeauro ra.org/security- builetin/20 19/07/11 / july-2019- code- aurora- security- builetinhttps://ww wcodeauro ra.org/security- builetin0ut-of- bounds Read25-07-201910Possible out of bound read occurs while processing beac oning request due to lack of check on action frames received from user controlled snapdragon Mobile, Snapdragon Mobile, S	Weakness	Publish Date	CVSS	Description & CVE I	D Patch	NCIIPC ID
Out-of- bounds25-07-20197.8playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & undestrial 107, Snapdragon Voice & m.com/co				710 / SD 670, SD 820A, / SD 850, SDM660, SDX	SD 845 20	
Out-of- bounds Read25-07-201910occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, 	bounds	25-07-2019	7.8	playing h265 video file denial of service issue in Snapdragon Auto, Snap Compute, Snapdragon Connectivity, Snapdrag Consumer IOT, Snapdra Industrial IOT, Snapdra Mobile, Snapdragon Voi Music, Snapdragon Wea in MSM8909W, QCS605 Qualcomm 215, SD 210 212/SD 205, SD 425, SI SD 430, SD 435, SD 439 429, SD 450, SD 625, SD 650/52, SD 665, SD 675 712 / SD 710 / SD 670, SD 820, SD 845 / SD 85 855, SD 8CX, SDM439, Snapdragon_High_Med_ SXR1130	leads to n dragon on agon gon ice & arables 5, /SD 0 427, /SD 0 427, /SD 5, SD 5, SD SD 730, 0, SD _2016,	O-QUA-SD_8-
	bounds	25-07-2019	10	occurs while processing beaconing request due of check on action fram received from user cont space in Snapdragon Au Snapdragon Consumer Electronics Connectivity Snapdragon Mobile, Snapdragon Voice & Mu MDM9607, MSM8996A QCA6174A, QCA6574A	g https://ww to lack w.codeauro es ra.org/secu rity- ito, bulletin/20 19/07/01/ y, july-2019- IOT, code- aurora- security- U, bulletin U, bulletin	O-QUA-SD_8-
	CV Scoring So (CVSS)	cale 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 & CVE ID					tch	NCIIP	CID
				675, SI SD 730 850, SI	5, SD 63 D 712 / S), SD 820 D 855, SI 50, SDX2	SD 710 / OA, SD 84 OM630,					
				CVE ID) : CVE- 2	2019-22	76				
Out-of- bounds Read	22-0	7-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2277				w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Authentica tion	25-0	7-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 CVE ID : CVE-2019-2278				w.cod ra.org rity-	019- a- ity-	0-QUA- 130819	/1766
Improper Restriction	22-0	7-2019	7.5	Shared memory gets updated with invalid data and may lead			-	//ww eauro	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1 1-2 2-3 3-4			le 0-1 1-2 2-3 3-4 4-5 5-6			2-3 3-4 4-5 5-6				9-10

Weakness	Publish D	ate	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
of Operations within the Bounds of a Memory Buffer				memor Snapdr Snapdr Snapdr Snapdr Snapdr MDM9 MDM9 MDM9 MDM9 MSM89 QCS40 215, SI SD 425 450, SI SD 425 710 / S SD 820 850, SI SDM63 SDX24, Snapdr	ss beyor sy. in Sna agon Co agon Co agon Mo agon W 150, MD 650, MS 996AU, (5, QCS6(0, 210/SI 5, SD 439 0, SD 44 1, SD 439 0, SD 44 1, SD 439 0, SD 44 1, SD 44	apdrago nnectiv nsumer dustrial obile, nice & M earables M9607, M8909V QCA6574 D5, Quale D 212/S D 730, S S SD 712 S S S D 84 D 730, S	rity- bullet	a- ity-			
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-20	919	4.6	image of memor cause e code. in Snapdr Snapdr Snapdr Snapdr QCS409 665, SI SD 670 835, SI SD 8CX SDM66	oice & M 05, SD 63	to ntly erified ompute, ity, IOT, IOT, USIC in 36, SD 5D 710 / 0, SD 5D 855, 30, 130	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-	1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereferenc e	25-07-2019	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1769	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1770
CV Scoring So (CVSS)	cale 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	escriptic	on & CVE	Pa	tch	NCIIP	C ID	
			210/SD SD 427, 439 / SI SD 632, 675, SD SD 730, 835, SD SD 8CX, SDM630 Snapdra SXR113 CVE ID	SD 430 D 429, S SD 636 712 / S SD 820 845 / S SDA66 D, SDM6 agon_Hi 0), SD 435 SD 450, 5 SD 710 / J, SD 820 SD 850, 5 0, SDM4 560, igh_Med	5, SD SD 625, 5, SD SD 670, 0A, SD SD 855, 139, _2016,				
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race con DMA bu Snapdra Connect Consum Industri	ndition ffer in j agon Au tivity, S her IOT, ial IOT, Snapdr 8909W , SD 42 435, SI 435, SI SD 712 820, SI 820, SI / SD 85), SDX2	while a ipeg driv ito, Snap napdrag Snapdra Snapdra Snapdra (Snapdra S, SD 42 (SD 450, SI (SD 450, SI (SD 71 (SD 71 (SD 71 (SD 71 (SD 71 (SD 71 (SD 71 (SD 71 (SD 72))	ccessing ver in odragon agon agon earables 996AU, 7, SD D 625, 10 / SD SD 835, 60, 4	w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD				w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	_
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346		
			Improper validation for inputs received from firmware can		
Out-of- bounds Write	22-07-2019	7.5	received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1773
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019-	O-QUA-SD_8- 130819/1774
CV Scoring So (CVSS)	cale 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	Pat	tch	NCIIPC ID			
			Snapdragon In Snapdragon M Snapdragon W MDM9206, MD MDM9640, MD MSM8909W, M QCS605, SD 42 430, SD 435, SI SD 636, SD 650 SD 710 / SD 67 820A, SD 835, 3 850, SDM660, 3 Snapdragon_H CVE ID : CVE-2	obile, earables in 0M9607, 0M9650, 1SM8996AU, 5, SD 427, SD 0 450, SD 625, 0/52, SD 712 / 70, SD 820, SD SD 845 / SD SDX20, SDX24, igh_Med_2016	code- auror securi bullet	ity-			
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound a due to buffer c checking size o from WLAN fir Snapdragon Au Consumer IOT, Industrial IOT, Mobile, Snapdu Music in MDM9 MDM9650, MS QCA6574AU, Q SD 210/SD 212 425, SD 427, SI SD 450, SD 625 665, SD 712 / S SD 730, SD 820 845 / SD 850, S SDM630, SDM6 SDX24 CVE ID : CVE-2	d https: w.cod ra.org rity- bullet 19/06 june-2 code- auror 0, securi bullet	a- ity-	0-QUA- 130819			
Use After Free	25-07-2019	4.6	Pointer derefer freeing IFE res lack of length o resource. in Sn Consumer IOT Industrial IOT,	ources due to check of in port apdragon , Snapdragon	w.cod ra.org rity- bullet	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/		0-QUA-SD_8- 130819/1776	
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 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 Wearable in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 SD 850, SD 855, SDM630, SDM660, SDX24	aurora- security- bulletin		
Use After Free	25-07-2019	4.6	CVE ID : CVE-2019-2293 Protection is missing while accessing md sessions info vi macro which can lead to use after-free in Snapdragon Aut Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298	b, https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1777	
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-craft command supplied by a userspace application. in Snapdragon Auto, Snapdrago Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	ed w.codeauro ra.org/secu rity-	0-QUA-SD_8- 130819/1778	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networkin in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20 SDX24		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2299 Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdrago Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wire Infrastructure and Networkir in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429 SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 67 SD 820A, SD 845 / SD 850, SE 855, SDM439, SDM660, SDX2 CVE ID : CVE-2019-2301	n https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin 0,	0-QUA-SD_8- 130819/1779
Out-of- bounds	25-07-2019	7.5	Out of bound access when reason code is extracted from	https://ww w.codeauro	100010/1000
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID		Ра	tch	NCIIP	CID		
Read			frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305				rity-	:019- a- ity-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675,			https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin		0-QUA-SD_8- 130819/1781		
CV Scoring Scale (CVSS)				,						

	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20		
			CVE ID : CVE-2019-2306		
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1782
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code-	0-QUA-SD_8- 130819/1783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308	aurora- security- bulletin	
Out-of- bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2309	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1784
Improper Restriction	25-07-2019	4.6	When handling the vendor command there exists a	https://ww w.codeauro	0-QUA-SD_8- 130819/1785
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 1010	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	
sd_855_firm	iware				
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1786
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIP	C ID
			MDM9 MSM89 QCA65 QCA65 QCA93 QCA98 QCN55 SD 210 425, SI SD 675 670, SI SD 835 855, SI SDM63	M9607, M9650, QCA617 6574, CA6584 CA8081 9379, Q 9886, Q 9886, Q 404, QC 2/SD 20 D 625, S 2/SD 7 D 820, S 5/SD 8! DA660, 560, SD2	4A, 4A, CA9531, CA9980, S605, 5, SD D 636, 10 / SD D 820A, 50, SD					
Improper Input Validation	25-07-2019	2.1	SDX24, SXR1130 CVE ID : CVE-2019-2240 While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD				w.qua m.con duct- secur ulletin	n/co y/pro ity/b ns	0-QUA- 130819	/1787
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3	3-4 1012	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660 SDM630, SDM660, SDX24, SXR1130	,	
			CVE ID : CVE-2019-2241		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosur in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SE 730, SD 820, SD 820A, SD 835 SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 CVE ID : CVE-2019-2243	e. https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1788
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with corrupted comment block. in Snapdragon Auto, Snapdrago Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	w.qualcom	0-QUA-SD_8- 130819/1789
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1790
CV Scoring So	cale 0-1	1-2	2-3 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, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1791
			CVE ID : CVE-2019-2260 Unauthorized access from GPU		
N/A	22-07-2019	4.9	subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1792
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
(0033)			1015		

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	Pa	tch	NCIIF	PC ID	
			Snapdr Snapdr Snapdr Infrastr in IPQ8 MDM92 QCA808 215, SD SD 425, 435, SD SD 425, 435, SD SD 625, 650/52 710 / S SD 820, 850, SD SDM43 Snapdr SXR113							
				: CVE-2						
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269				ra.org rity-	eauro s/secu in/20 5/03/ 2019- a- ity-	0-QUA- 130819	_
Out-of-	25-07-2019	7.8	IOMMU page fault while				https:	//ww	O-QUA-	SD_8-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

bounds Read			playing h265 video file leads to	w.qualcom	130819/1794
			denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2273	m.com/co mpany/pro duct- security/b ulletins	
Out-of- bounds 2 Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	O-QUA-SD_8- 130819/1795

(CVSS)	0-1	1-2	2-3	3-4 1017	. 5	0-5	0-7	/-ð	8-9	9-10
CV Scoring Scale	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 & CVE ID					tch	NCIIP	C ID
				CVE ID : CVE-2019-2276							
Out-of- bounds Read	22-0	7-2019	4.6	due to termin data in Auto, S Snapdn Snapdn Snapdn Snapdn MSM89 QCS60 205, SI SD 435 636, SI SD 710 820A, S 850, SI SDM66	WLAN i mapdrag ragon Co ragon In ragon Vo 996AU, (996AU, (996AU, 5 96AU, 5 9	IULL user co n Snapd gon Com onsumer dustrial obile, oice & Mi QCS405, 0/SD 21 0 427, SI 0/SD 625 0 675, SI 70, SD 625 0 675, SI 70, SD 73 SD 845 / DA660, S 4	ntrolled Iragon pute, IOT, IOT, usic in 2/SD D 430, 5, SD D 712 / 80, SD / SD SDM630,	w.cod ra.org rity- bullet 19/00 june-2 code- auror secur bullet	a- ity-	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-0'	7-2019	7.5	Shared with in to acce memor Snapdn Snapdn Snapdn Snapdn Snapdn MDM9 MDM9 MDM9 MSM84 QCS40 215, SI SD 425 450, SI SD 665 710 / S	y gets uj ta and n nd the al apdrago onnectivi onsumer dustrial	pdated nay lead located n Auto, ity, IOT, IOT, USIC, in V, 4AU, comm D 205, 29, SD D 636, 2 / SD SD 820,	w.cod ra.org rity- bullet 19/06	a- ity-	0-QUA- 130819	_	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptic	on & CVE	Pa	tch	NCIIP	PC ID	
			SDM63 SDX24 Snapdr	0 855, SI 0, SDM6 , ragon_Hi 9 : CVE-2	560, SDX igh_Med					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	image of memoricause of code. in Snapdr Snapdr Snapdr Snapdr Snapdr QCS40. 665, SI SD 670 835, SI SD 8CX SDM66	uthentio can be lo cy and su execution n Snapdh ragon Co ragon Co ragon Mo ragon Mo ragon Mo 5, QCS60 0 675, SI 0, SD 730 0 845 / S 2, SDA66 50, SDX2	baded in ubseques n of unv ragon Co onnectivi onsumer dustrial obile, oice & Mi 05, SD 63 0, SD 820 50 712 / S 0, SD 820 50 850, S 0, SDM6 4, SXR12	to ntly erified ompute, ity, IOT, IOT, IOT, SD 710 /), SD SD 855, 530, 130	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
NULL Pointer Dereferenc e	25-07-2019	7.8	happer with w Snapdr Compu Consur Industr IoT, Sn Snapdr MDM9 MDM9 MDM9 MSM89 QCS40 215, SI SD 425 435, SI	n when p rong blo ragon Au ite, Snap ner IOT, rial IOT, apdrago ragon W 150, MD 607, M	olaying t ock grou ito, Snap dragon Snapdra on Mobil oice & Mi earables M9206, M9650, SM8996 D5, Qualo D 212/S 7, SD 430 SD 429, S	p id in odragon agon e, usic, s in 5AU, comm D 205,), SD	w.qua m.cor	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2334		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1800
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct-	0-QUA-SD_8- 130819/1801
CV Scoring So (CVSS)	cale 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	on & CVE	Ра	tch	NCIIP	PC ID	
	Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 CVE ID : CVE-2019-2346 Improper validation for inputs						secur ulleti			
Out-of- bounds Write	22-07-2019	7.5	Impropreceive lead to issue in Snapdu Compu Consur Indust Mobile Music, in MDM MDM9 MDM9 MDM9 MDM9 MSM84 QCS40 215, SI SD 425 435, SI SD 625 665, SI SD 670 820A, SI	per valid ed from 1 an out o ragon Au re, Snap mer IOT, rial IOT, Snapdra M9150, M 607, MD 650, MS 996AU, 0 5, QCS60 0 210/SI 5, SD 427 0 439 / S 5, SD 632 0 675, SI 0, SD 730 SD 835, SI 80, SDM6	lation fo firmwar of bound driver. ir uto, Snap dragon Snapdra Snapdra Snapdra agon We MDM920 M9640, M8909V QCA6574 D9640, M8909V QCA6574 D5, Qual D 212/S 7, SD 430 SD 429, S 2, SD 636 D 712 / S 0, SD 820 SD 845 / DA660, S	r inputs e can l write odragon agon agon oice & arables 06, V, 4AU, comm D 205, 0, SD SD 450, 5, SD SD 450, 5, SD SD 710 / 0, SD (SD SDM439,	w.cod ra.org rity- bullet 19/00 june-2 code- auror secur bullet	a- ity-	0-QUA- 130819	_
CV Scoring Sc	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

0-1	1-2

(CVSS)

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2019-2287			
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2292	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1803	
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2293	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1804	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-	https://ww w.qualcom m.com/co	O-QUA-SD_8- 130819/1805	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298	mpany/pro duct- security/b ulletins	
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 /	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1806
CV Scoring So (CVSS)	cale 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	PC ID
			SD 670, SD 730 820A, SD 835, S 850, SD 855, SD SDX24	SD 845 / SD				
			CVE ID : CVE-2	019-2299				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of ou read if id receiv not in range of Snapdragon Au Compute, Snap Consumer IOT, Industrial IOT, Mobile, Snapdr Wearables, Sna Infrastructure a in IPQ4019, IPC MSM8909W, M QCA9980, QCS6 215, SD 425, SD SD 450, SD 625 636, SD 712 / S SD 820A, SD 84 855, SDM439, S CVE ID : CVE-2	https:, w.code ra.org rity- bulleti 19/07 july-20 code- aurora securi bulleti	eauro /secu n/20 /01/ 019- a- ty-	0-QUA- 130819		
Out-of- bounds Read	25-07-2019	7.5	Consumer Elect Connectivity, Si Consumer IOT, Industrial IOT, Mobile, Snapdr Music in MDM9 MDM9206, MD MDM9640, MD MSM8996AU, Q QCA6574AU, Q	extracted from nout validating h in to, Snapdragon tronics napdragon Snapdragon agon Voice & 0150, M9607, M9650, QCA6174A,	https:, w.code ra.org rity- bulleti 19/07 july-20 code- aurora securi bulleti	eauro /secu n/20 /01/ 019- a- ty-	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2305		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2306	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1809
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019-	0-QUA-SD_8- 130819/1810
CV Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

N/A 25-07-2019 7.2 MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, 19/07/01/ july-2019- code- aurora- security- bulletin 130819/181	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A25-07-20197.27.2potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435,https://ww w.codeauro ra.org/secu rity- bulletinN/A0-QUA-SD_8 130819/181				Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24	aurora- security-	
SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630,	N/A	25-07-2019	7.2	potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855,	w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	0-QUA-SD_8- 130819/1811
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1	-	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			•	Patch	NCIIPC ID
			SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-2308		
within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SD_8- 130819/1812
sdx20_firmw	vare				
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDX2- 130819/1813
CV Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9650, MDM9640, MDM9650, MSM8996AU, QCA6174A,	https://w w.qualcom m.com/co mpany/pr duct- security/h ulletins	n O-QUA-SDX2- 130819/1814
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	-8 8-9 <mark>9-1</mark> 0

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 CVE ID : CVE-2019-2253	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SDX2- 130819/1815
CV Scoring So (CVSS)	cale 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	Pa	tch	NCIIP	C ID
Informatio n Exposure	25-07-2019	7.5	accuration accuration of the second s	ngly deci ation in napdrag ragon Co ragon Io ragon Co ragon Co	be degra oded Snapdra gon Com nsumer dustrial F, Snapd agon Vo gon We ADM920 M9615, M9635N M9650, M9635N M9650, M8909V QCS605, SD 210 O 425, SI CSD 210 O 425, SI CSD 439 O 615/10 O 632, SI 665, SD SD 670, A, SD 83 SD 855, S 39, SDM 0, gh_Med	ded due agon pute, IOT, IOT, Iragon bice & arables 06, M, V, V,)/SD D 427, 0 / SD 0 427, 0 / SD 6/SD 0 636, 675, SD 50 8CX, 1630, _2016,	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206,			w.cod ra.org rity- bullet	a-	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3					7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCIIF	PC ID
			MDM9 QCS40 215, SI SD 425 435, SI SD 625 665, SI SD 730 845 / S SDM43 SDX20 Snapdi SXR11		M8909V D5, Qualo D 212/S 7, SD 430 SD 429, S SD 429, S SD 710 / DA, SD 83 SD 855, 530, SDM	bullet	in			
Use After Free	25-07-2019	4.6	Access happer diag dr free iss Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Infrast in IPQ4 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 MDM9 SM89 QCA95 210/SI SD 427 450, SI 650/52 670, SI SD 845 SDX20	CVE ID : CVE-2019-2260 Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016		w.coc ra.org rity- bullet	a- ity-	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow w processing the high level lii process action frame due to improper buffer length validation in Snapdragon A Snapdragon Compute, Snapdragon Consumer IOT Snapdragon Industrial IOT Snapdragon Mobile, Snapdragon Voice & Music MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SI 665, SD 712 / SD 710 / SD SD 730, SD 820, SD 820A, S 835, SD 845 / SD 850, SD 8 SDA660, SDM630, SDM660 SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269	im o Auto, f, c, in bulletin/20 in code- b aurora- 670, security- bulletin june-2019- code- b aurora- 670, security- bulletin	0-QUA-SDX2- 130819/1819
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur i display function due to lack validation of header block is set by user. in Snapdragon Auto, Snapdragon Consume IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 422 SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SI 636, SD 650/52, SD 712 / S 710 / SD 670, SD 820A, SD / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2272	k of size https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin SD bulletin	0-QUA-SDX2- 130819/1820
Improper	22-07-2019	7.5	Shared memory gets updat	ted https://ww	0-QUA-SDX2-
CV Scoring So (CVSS)	cale 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 & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279	w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	130819/1821
NULL Pointer Dereferenc e	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDX2- 130819/1822
CV Scoring Sc					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			SD 600, SD 615/16/SD 415, S 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SE 670, SD 730, SD 820, SD 820, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016				
			CVE ID : CVE-2019-2334				
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	25-07-2019	4.4	Race condition while accessin DMA buffer in jpeg driver in Snapdragon Auto, Snapdrago Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearabl in MSM8909W, MSM8996AU QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SE 670, SD 820, SD 820A, SD 833 SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2345	n https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora-			
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inpur received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdrago Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearable in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019-			
CV Scoring So		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439 SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2287		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2290	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDX2- 130819/1825
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora-	0-QUA-SDX2- 130819/1826
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24	security- bulletin	
Use After Free	25-07-2019	4.6	CVE ID : CVE-2019-2292 Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDX2- 130819/1827
Integer Overflow or Wraparou nd	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code-	O-QUA-SDX2- 130819/1828
CV Scoring So	cale 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	Ра	tch	NCIIF	CID
			Industri Mobile, Music, S Infrastr in IPQ40 IPQ807 MDM92 MDM96 MSM89 QCA657 QCA937 SD 210, 425, SD SD 210, 425, SD SD 450, 636, SD SD 450, 636, SD SD 670, 820A, S 850, SD SDX24 CVE ID	auror secur bullet	ity-					
Out-of- bounds Read	25-07-2019	7.5	reason of frame d the fram Snapdra Consum Consum Industri Mobile, Music ir MDM92 MDM96 MSM89 QCA657 QCA937 425, SD SD 450, 665, SD	CVE ID : CVE-2019-2299 Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD				c//ww leauro g/secu cin/20 7/01/ c019- a- ity- cin	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	<mark>3-4</mark> 1037	4-5	5-6	6-7	7-8	8-9	9-10

	Publish Date	CVSS	Description & CVE I	D Patch	NCIIPC ID
			850, SD 855, SDA660, S SDM660, SDX20, SDX24		
			CVE ID : CVE-2019-23		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of striwhile handling the buffer to out of bound read in in Snapdragon Auto, Snapdragon Connectivit Snapdragon Consumer Snapdragon Industrial I Snapdragon IoT, Snapd Mobile, Snapdragon Vot Music, Snapdragon Weat in MDM9150, MDM920 MDM9607, MDM9650, MSM8909W, MSM8996 QCS405, QCS605, Qualc 215, SD 210/SD 212/SI SD 425, SD 427, SD 430 435, SD 439 / SD 429, S SD 615/16/SD 415, SD 632, SD 636, SD 665, SD SD 712 / SD 710 / SD 6 730, SD 820, SD 820A, S SD 845 / SD 850, SD 85 SDA660, SDM439, SDM SDM660, SDX20 CVE ID : CVE-2019-23	er leads display ty, IOT, IOT, ragon https://ww w.codeauro ra.org/secu rity- bulletin/20 6, rity- bulletin/20 6AU, 19/07/01/ comm july-2019- 0 205, SD aurora- security- bulletin 0 675, 70, SD SD 835, 5, 630,	0-0114-SDX2-
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underf due to lack of validation calculation of data leng 802.11 Rx management configuration in Snapdr Auto, Snapdragon Cons Electronics Connectivit Snapdragon Consumer Snapdragon Industrial Snapdragon Mobile, Snapdragon Voice & Mu MDM9150, MDM9206,	n before th in ra.org/secu rity- ragon umer y, IOT, IOT, inttps://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security-	0-011A-SDX2-
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2307		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDX2- 130819/1832
Out-of- bounds	25-07-2019	7.5	While storing calibrated data from firmware in cache, An	https://ww w.codeauro	0-QUA-SDX2- 130819/1833
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 1039	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 CVE ID : CVE-2019-2309	ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	
sxr1130_fir	mware		CVEID. CVE-2019-2309		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SXR1- 130819/1834
CV Scoring S	calo				

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				1040)					

Weakness	Publ	ish Date	CVSS	C	escriptio	on & CVE	ID	Pat	ch	NCIIP	CID
				SD 450 636, SD SD 820 845 / S SDM43	, SD 625) 712 / S , SD 820 D 850, S 9, SDM6 agon_Hi	D 439 / S 5, SD 632 SD 710 / OA, SD 83 SD 8CX, S 530, SDM igh_Med					
				CVE ID	: CVE-2	2019-22	35				
NULL Pointer Dereferenc e	25-0'	7-2019	2.1	during termina applica Auto, Si Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Infrastr in IPQ8 MDM96 QCA809 215, SD 427, SD 427, SD 632, SD 675, SD SD 730 835, SD SDM43 Snapdr	secure a ation us tion ids napdrag agon Co agon Co agon Co agon Co agon M agon M agon W cucture 074, MI 607, MD 655, MS 81, QCS 0410/12 0430, SI 0430, SI 0430, SI 055, MS 81, QCS 0410/12 0430, SI 055, MS 81, QCS 0410/12 0430, SI 0430, SI 055, MS 81, QCS 0410/12 0430, SI 0430, SI 0430, SI 0430, SI 055, SD 820 0430, SI 055, SD 820 0430, SI 055, SD 820 055, SD 820 050 055, SD 820 050 050 050 050 050 050 050 050 050 0	nice & Mi ired and Net DM9206 M9650, M8996A 605, Qua 2, SD 42 D 435, SI 0, SD 625 D 650/5 SD 710 / 0, SD 820	on ific odragon pute, ity, ity, IOT, IOT, USIC, working , U, alcomm 5, SD D 439 / 5, SD 2, SD 2, SD 2, SD 2, SD 3 SD 670, DA, SD 4660, _2016,	https:, w.qua m.com mpany duct- securi ulletin	lcom 1/co y/pro ty/b	0-QUA- 130819	
N/A	25-0	7-2019	2.1		Failure in taking appropriate action to handle the error case				//ww lcom	0-QUA- 130819	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237	m.com/co mpany/pro duct- security/b ulletins	
Out-of- bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2238	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SXR1- 130819/1837
Improper Input	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI	https://ww w.qualcom	0-QUA-SXR1- 130819/1838
CV Scoring Sc (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 1042	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SE 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SE 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239	security/b ulletins g	
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	m.com/co mpany/pro	0-QUA-SXR1- 130819/1839
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SXR1- 130819/1840
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 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 MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130		
			CVE ID : CVE-2019-2241		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDX20, Snapdragon_High_Med_2016,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SXR1- 130819/1841
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130		
			CVE ID : CVE-2019-2254		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9206, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2260	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SXR1- 130819/1842
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SXR1- 130819/1843
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
(CVSS)			1046		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2261		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2269	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	O-QUA-SXR1- 130819/1844
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon	https://ww w.qualcom m.com/co mpany/pro	O-QUA-SXR1- 130819/1845
CV Scoring So (CVSS)	cale 0-1	1-2	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
			Compute, Snapdr Connectivity, Sna Consumer IOT, S Industrial IOT, S Mobile, Snapdrag Music, Snapdrag in MSM8909W, O Qualcomm 215, S 212/SD 205, SD 4 SD 430, SD 435, S 429, SD 450, SD 6 650/52, SD 665, 712 / SD 710 / S SD 820, SD 845 / 855, SD 8CX, SDM Snapdragon_Hig SXR1130 CVE ID : CVE-20	apdragon inapdragon napdragon gon Voice & on Wearables QCS605, SD 210/SD 425, SD 427, SD 439 / SD 625, SD SD 675, SD SD 675, SD D 670, SD 730, / SD 850, SD M439, h_Med_2016,	duct- securi ulletin	• •		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	CVE ID : CVE-2019-2273 An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2281		https:, w.qua m.com mpany duct- securi ulletin	lcom l/co 7/pro ty/b	0-QUA- 130819	
Improper Restriction of Operations within the	25-07-2019	2.1	Out of bound real information disc firmware due to checking of an er structure that ca	https:, w.quai m.com mpany duct-	lcom I/co	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 1048	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descrip	otion & CVE	ID	Pa	tch	NCIIP	PC ID
Bounds of a Memory Buffer			a kernel driv Auto, Snapd Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon MSM8909W QCS605, Qua 210/SD 212 SD 427, SD 4 439 / SD 429 SD 632, SD 6 675, SD 712 SD 730, SD 6 835, SD 845 SD 8CX, SDA SDM630, SD Snapdragon SXR1130 CVE ID : CVI	ragon Com Connectivi Consumer Industrial Mobile, Voice & Mi Wearables (, MSM8996 alcomm 21 /SD 205, Si 30, SD 450, Si 36, SD 450, Si 36, SD 665 / SD 710 / B20, SD 820 / SD 850, Si 660, SDM4 M660, _High_Med	pute, ity, IOT, IOT, is in 5AU, 5, SD D 425, 5, SD SD 625, 5, SD SD 670, 0A, SD SD 855, 39, _2016,	secur	• •		
sd_8cx_firm	ware					<u> </u>		<u> </u>	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404,		w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	—	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

	3-4	4-5						
1010								

Weakness	Publis	h Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
				QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2235							
NULL Pointer Dereferenc e	25-07	-2019	2.1	Null po during termin applica Auto, S Snapdn Snapdn Snapdn Snapdn Snapdn Snapdn Snapdn Infrast in IPQ& MDM9 QCA80 215, SI 427, SI SD 429 632, SI 675, SI SD 730 835, SI SDM43 Snapdn SXR113	ointer de secure a ation us napdrag ragon Co ragon Co ragon Co ragon Co ragon Mo ragon W ructure 3074, MI 607, MD 655, MS 81, QCS 0 410/12 0 430, SI 0 430, SI 0 430, SI 0 50 450 0 636, SI 0 712 / S 0 8CX, SI 69, SD M6 ragon_Hi 30	ereferend application ing spectors in Snap gon Componective onsumer onsumer dustrial obile, oice & M ired and Net DM9206 0M9650, M8996A 605, Qua 2, SD 42 D 435, SI 0, SD 625 D 650/5 SD 710 / 0, SD 820	ce on ific odragon pute, ity, ity, IOT, IOT, IOT, usic, working , U, alcomm 5, SD 2, SD 2, SD 2, SD 2, SD 2, SD 3, SD 2, SD 439 / 5, SD 2, SD 4, SD 2, SD 4, SD 5, SD 4, SD 4, SD 5,	w.qua m.cor mpan duct- secur ulletin	n/co y/pro ity/b	0-QUA- 130819	
CV Scoring So (CVSS)	cale	0-1	1-2	2-3	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	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2237	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_8- 130819/1850
Out-of- bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop- expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 CVE ID : CVE-2019-2238	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SD_8- 130819/1851
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networkin in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SI 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, S 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239	g https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1852
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	mpany/pro duct-	0-QUA-SD_8- 130819/1853
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 1052	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIF	PC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6564, QCA6574, QCA6584AU, QCA8081, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9380, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240				
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https:/ w.qual m.com mpany duct- securit ulletin	lcom l/co 7/pro ty/b	0-QUA- 130819	
CV Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2241		
Informatio n Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630,	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1855
CV Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2254		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDM439, S	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1856
Out-of- bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1857
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 73 SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130		
			CVE ID : CVE-2019-2273		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855 SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2281	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SD_8- 130819/1858
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	auct-	0-QUA-SD_8- 130819/1859
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 1056	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descriptio	on & CVE ID	Pa	tch	NCIIF	PC ID
			Snapdragon Co Snapdragon In Snapdragon M Snapdragon W Snapdragon W MSM8909W, M QCS605, Qualc 210/SD 212/S SD 427, SD 420, S SD 632, SD 636 675, SD 712 / S SD 730, SD 820 835, SD 845 / S SD 8CX, SDA66 SDM630, SDM6 Snapdragon_H SXR1130 CVE ID : CVE-2	dustrial IOT, obile, oice & Music, earables in ISM8996AU, omm 215, SD D 205, SD 425, D 205, SD 425, SD 450, SD 625 5, SD 665, SD SD 710 / SD 67 0, SD 820A, SD SD 850, SD 855 50, SDM439, 660, igh_Med_2016	5, 10, 5,			
Improper Validation of Array Index	25-07-2019	7.2	Firmware is ge of overwriting scan command host because o validation. in S Compute, Snap Consumer IOT, Industrial IOT, Mobile, Snapdra Infrastructure in IPQ8074, QC QCS404, QCS40 425, SD 427, SI SD 450, SD 625 712 / SD 710 / SD 835, SD 8CX, SI	CVE ID : CVE-2019-2343 Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660			0-QUA- 130819	
sdx24_firm	ware							
CV Scoring So								

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2239	w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDX2- 130819/1861
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	0-QUA-SDX2- 130819/1862
CV Scoring So (CVSS)	cale 0-1	1-2	Connectivity, Snapdragon 2-3 3-4 4-5 5-6 1058	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6564, QCA6574, QCA6584AU, QCA8081, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://w w.qualcon m.com/co mpany/pr duct- security/t ulletins	n O-QUA-SDX2- 130819/1863
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 CVE ID : CVE-2019-2241		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDX2- 130819/1864

C	V Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
					1060)					

Weakness	Publish Date	CVSS	Description & CVE ID				Ра	tch	NCIIF	PC ID
			CVE ID : CVE-2019-2260							
NULL Pointer Dereferenc e	22-07-2019	4.6	occurs while o Snapdr Consun Mobile, Music, 3 in MDM MSM89 SD 425 435, SE SD 625 712 / S 820A, S 820A, SE SDM66	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2264				//ww leauro g/secu in/20 6/03/ 2019- a- ity- in	0-QUA- 130819	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	process process improp validati Snapdr Snapdr Snapdr Snapdr Snapdr MDM92 QCS605 665, SD SD 730 835, SD SDA660	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130			w.cod ra.org rity- bullet	a- ity-	0-QUA- 130819	
Out-of- bounds	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack			w.cod	//ww leauro g/secu	0-QUA- 130819		
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 1061	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID			Pat	ch	NCIIP	CID
Read			of check on act received from space in Snapo Snapdragon Co Electronics Co Snapdragon M Snapdragon M Snapdragon M MDM9607, MS QCA6174A, QC QCA9377, QCA QCS605, SD 63 675, SD 712 / SD 730, SD 820 850, SD 855, S SDM660, SDX2	rity- bullet 19/07 july-2 code- aurora securi bullet	//01/ 019- a- ty-				
Out-of- bounds Read	22-07-2019	4.6	CVE ID : CVE-2019-2276 Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24		https: w.cod ra.org rity- bullet 19/06 june-2 code- aurora securi bullet	eauro /secu in/20 6/03/ 2019- a- ty-	0-QUA- 130819		
Improper Restriction of Operations	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto,			https: w.cod ra.org rity-	eauro	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 106	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pat	tch	NCIIP	CID
within the Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2279				bullet 19/06 june-2 code- auror securi bullet	2019- a- ity-		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	image c memor cause e code. in Snapdr Snapdr Snapdr Snapdr Snapdr QCS405 665, SD SD 670, 835, SD SD 8CX SDM66	uthentic can be lo y and su xecution a Snapdr agon Con agon Con agon Mo agon Mo agon Mo 5, QCS60 675, SD 675, SD 675, SD 675, SD 675, SD 845 / S , SDA660 0, SDX2 ² : CVE-20	aded in bseques of unver agon Co nnectivi nsumer lustrial bile, ice & Mu 5, SD 63 0 712 / S , SD 820 D 850, S 0, SDM6 4, SXR12	to ntly erified ompute, ity, IOT, IOT, IOT, SD 710 /), SD SD 855, 30, 130	w.qua m.con	n/co y/pro ity/b	0-QUA- 130819	
Concurrent Execution	25-07-2019	4.4		ndition affer in j		ccessing ver in	-	//ww eauro	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4 1063	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchroniz ation ('Race Condition')			Connectivity, SnapdragonrConsumer IOT, SnapdragonbIndustrial IOT, Snapdragon1Mobile, Snapdragon Wearablesjuin MSM8909W, MSM8996AU,cQCS605, SD 425, SD 427, SDa430, SD 435, SD 450, SD 625,s	ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	
Out-of- bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24Improvements Compute, SD SD 2000000000000000000000000000000000000	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/06/03/ june-2019- code- aurora- security- bulletin	0-QUA-SDX2- 130819/1872
Use After	25-07-2019	4.6	Multiple open and close from h	https://ww	0-QUA-SDX2-
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 6 1064	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	ID	Ра	tch	NCIIP	CID
Free			camera destroy in Snapdu Snapdu Snapdu Snapdu Snapdu MDM9 MDM9 MSM84 QCS60 430, SI SD 636 SD 710 820A, SI S50, SI Snapdu	le thread a driver t yed session odragon ragon Co ragon Co ragon Mo 206, MD 640, MD 640, MD 640, MD 5, SD 42 0, SD 650 0 / SD 650 0 / SD 67 SD 835, SI 5, SD 650 0 / SD 67 SD 850 SD 8	to access ion data Auto, innective dustrial obile, earables M9607, M9650, SM8996 5, SD 42 O 450, SI 0, SD 82 O 450, SI 0, SD 82 SD 845 / SDX20, S igh_Med	ra.org rity- bullet	a- ity-	130819	/1873	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of due to checkin from W Snapdn Consur Industr Mobile Music i MDM9 QCA65 SD 210 425, SI SD 450 665, SI SD 730 845 / S SDM63	CVE ID : CVE-2019-2290 Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24				://ww leauro g/secu cin/20 6/03/ 2019- ca- ity- cin	0-QUA- 130819	
CV Scoring So (CVSS)	cale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2293	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDX2- 130819/1875
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use- after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2298	https://ww w.qualcom m.com/co mpany/pro duct- security/b ulletins	O-QUA-SDX2- 130819/1876
Integer Overflow or	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a	https://ww w.codeauro ra.org/secu	0-QUA-SDX2- 130819/1877
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparou nd			userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2299		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670	aurora- security- bulletin	0-QUA-SDX2- 130819/1878
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24		
			CVE ID : CVE-2019-2301		
Out-of- bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9206, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2305	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDX2- 130819/1879
Integer Underflow (Wrap or Wraparou nd)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640,	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDX2- 130819/1880
CV Scoring S (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24		
N/A	25-07-2019	7.2	CVE ID : CVE-2019-2307 User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 CVE ID : CVE-2019-2308	https://ww w.codeauro ra.org/secu rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin	0-QUA-SDX2- 130819/1881
Improper Restriction of	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due	https://ww w.codeauro ra.org/secu	0-QUA-SDX2- 130819/1882
CV Scoring So (CVSS)	cale 0-1	1-2	2-3 3-4 4-5 5-6 1069	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Operations within the Bounds of a Memory Buffer			to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 CVE ID : CVE-2019-2312	rity- bulletin/20 19/07/01/ july-2019- code- aurora- security- bulletin		
Tp-link						
archer_c120	0_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-07-2019	7.5	CMD_SET_CONFIG_COUNTRY in the TP-Link Device Debug protocol in TP-Link Archer C1200 1.0.0 Build 20180502 rel.45702 and earlier is prone to a stack-based buffer overflow, which allows a remote attacker to achieve code execution or denial of service by sending a crafted payload to the listening server	N/A	O-TPARCH- 130819/1883	
			CVE ID : CVE-2019-13614			
Zeroshell zeroshell						
Improper Neutralizat	19-07-2019	10	Zeroshell 3.9.0 is prone to a remote command execution	N/A	O-ZER-ZERO-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			vulnerability. Specifically, this issue occurs because the web application mishandles a few HTTP parameters. An unauthenticated attacker can exploit this issue by injecting OS commands inside the vulnerable parameters. CVE ID : CVE-2019-12725		130819/1884
ZTE	L			1	
otcp_firmwa	are				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	22-07-2019	2.3	All versions up to V1.19.20.02 of ZTE OTCP product are impacted by XSS vulnerability. Due to XSS, when an attacker invokes the security management to obtain the resources of the specified operation code owned by a user, the malicious script code could be transmitted in the parameter. If the front end does not process the returned result from the interface properly, the malicious script may be executed and the user cookie or other important information may be stolen. CVE ID : CVE-2019-3414	http://sup port.zte.co m.cn/supp ort/news/ LoopholeIn foDetail.as px?newsId =1010883	O-ZTE-OTCP- 130819/1885

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