

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

16 - 30 Sep 2021

Vol. 08 No. 18

Weakness	Publish Date	cvss	Description 8	& CVE ID	Pa	tch	NCII	PC ID
			Application	on				
activefusions								
order_status_	batch_chang	e						
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-21	4.3	Cross-site scripting vulnerability in O Batch Change Plut CUBE 3.0 series) allows a remote a inject an arbitrary unspecified vector CVE ID : CVE-202	order Status ag-in (for EC- all versions attacker to y script via ors.	N/A		A-ACT 06102	-ORDE- 1/1
activemedia								
microcopy								
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The edit function MicroCopy Word through 1.1.0 may request to fetch to option. The id particle or validated before to a SQL statement SQL injection.  CVE ID: CVE-202	N/A		A-ACT 06102	-MICR- 1/2	
Adobe								
creative_clou	d_desktop_ap	plicati	on					
Improper Input Validation	29-Sep-21	4.6	Adobe Creative C Desktop Applicat macOS version 5. earlier) is affected privilege escalation vulnerability that a normal user to OOBE directory a	x.adob /secur oducts ive-	//help be.com rity/pr s/creat /apsb2 html	A-ADO 06102	0-CREA- 1/3	
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pa	tch	NCI	IPC ID
			-	he adm	f any dir ninistrat					
			CVE ID	: CVE-2	2021-28	8547				
digital_edition	ns									
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	27-Sep-21	9.3	4.5.11.1 are affer comma vulnera authent leverage executed User into abusthat a umalicio	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary command execution vulnerability. An authenticated attacker could everage this vulnerability to execute arbitrary commands. User interaction is required to abuse this vulnerability in that a user must open a maliciously crafted .epub file.  EVE ID: CVE-2021-39826			https:/ x.adob /secur oducts al- Edition b21-80	e.com ity/pr i/Digit	A-AD0 06102	0-DIGI- :1/4
			CVE ID	: CVE-	2021-39	9826				
Creation of Temporary File in Directory with Insecure Permissions	27-Sep-21	6.8	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary file write vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to write an arbitrary file to the system. User interaction is required before product installation to abuse this vulnerability.  CVE ID: CVE-2021-39827			https:/x.adob /secur oducts al- Edition b21-80	e.com ity/pr i/Digit	A-ADC 06102	)-DIGI- :1/5	
Creation of Temporary File in Directory with Insecure Permissions	27-Sep-21	6.8	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by a privilege escalation vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to escalate privileges. User			https:/ x.adob /secur oducts al- Edition b21-80	e.com ity/pr i/Digit ns/aps	A-AD0 06102	)-DIGI- :1/6	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			produ	ction is r ct instal Ilnerabil	lation to					
			CVE II	) : CVE-	2021-39	9828				
experience_m	anager									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	4.3	version is affect vulner Conter auther send a requestible de Malicide execut brows the pay vulner	Experience of 6.5.9.0 cted by a cability was record as to achorous Java and a ced in a ver when a cable field as to achorous as to achorous Java and a contact and a conta	(and early then created POS ieve service. Script myictim's they braining the d.	arlier) XSS eating can ST ver- hay be cowse to	ience-	e.com ity/pr /exper er/aps	A-AD0 06102	O-EXPE- 21/7
Improper Input Validation	27-Sep-21	4	Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a improper input validation vulnerability via the path parameter. An authenticated attacker can send a malformed POST request to achieve serverside denial of service.  CVE ID: CVE-2021-40712				ience-	e.com ity/pr /exper er/aps	A-AD0 06102	)-EXPE- 21/8
Improper Certificate Validation	27-Sep-21	4.3	Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a improper certificate validation vulnerability in the cold storage component. If an attacker can achieve a man in the middle when the cold server establishes a new			ience-	e.com ity/pr /exper er/aps	A-AD0 06102	)-EXPE- 21/9	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certificate, they would be ab to harvest sensitive information.	le	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	4.3	Adobe Experience Manager version 6.5.9.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability via the accesskey parameter. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser	https://help x.adobe.com /security/pr oducts/exper ience- manager/aps b21-82.html	A-ADO-EXPE- 061021/10
incopy			CVE ID : CVE-2021-40714		
Access of Memory Location After End of Buffer	27-Sep-21	6.8	Adobe InCopy version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious TIFF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.  CVE ID: CVE-2021-39818	F - // - F	A-ADO-INCO- 061021/11
Access of Memory Location After End of Buffer	27-Sep-21	6.8	Adobe InCopy version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious XML file, potentially resulting in arbitrary code execution in the context of the current	x.adobe.com /security/pr	A-ADO-INCO- 061021/12
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			user. User interaction is required to exploit this vulnerability.		
			CVE ID : CVE-2021-39819		
indesign					
Out-of- bounds Read	29-Sep-21	6.8	Adobe InDesign versions 16.3 (and earlier), and 16.3.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious TIF file.  CVE ID: CVE-2021-39821	https://help x.adobe.com /security/pr oducts/indes ign/apsb21- 73.html	A-ADO-INDE- 061021/13
photoshop_20	)20				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Sep-21	9.3	Adobe Photoshop versions 21.2.11 (and earlier) and 22.5 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  CVE ID: CVE-2021-40709	https://help x.adobe.com /security/pr oducts/phot oshop/apsb2 1-84.html	A-ADO-PHOT- 061021/14
photoshop_20	)21				
Buffer Copy without	27-Sep-21	9.3	Adobe Photoshop versions 21.2.11 (and earlier) and 22.5	https://help x.adobe.com	A-ADO-PHOT- 061021/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			(and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  CVE ID: CVE-2021-40709	/security/pr oducts/phot oshop/apsb2 1-84.html	
premiere_ele	ments				
Access of Memory Location After End of Buffer	27-Sep-21	9.3	Adobe Premiere Elements version 2021.2235820 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious png file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.  CVE ID: CVE-2021-39824	https://help x.adobe.com /security/pr oducts/prem iere_element s/apsb21- 78.html	A-ADO- PREM- 061021/16
adonisjs					
edge					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-21	5.8	This affects the package edge.js before 5.3.2. A type confusion vulnerability can be used to bypass input sanitization when the input to be rendered is an array (instead of a string or a SafeValue), even if {{}} are	https://snyk. io/vuln/SNY K-JS-EDGEJS- 1579556, https://githu b.com/edge- js/edge/com mit/fa2c7fde 86327aeae2	A-ADO-EDGE- 061021/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used.  CVE ID: CVE-2021-23443	32752e89a6 e37e2e469e 21	
Ait-pro					
bulletproof_se	ecurity				
Exposure of Sensitive Information to an Unauthorize d Actor	17-Sep-21	5	The BulletProof Security WordPress plugin is vulnerable to sensitive information disclosure due to a file path disclosure in the publicly accessible ~/db_backup_log.txt file which grants attackers the full path of the site, in addition to the path of database backup files. This affects versions up to, and including, 5.1.  CVE ID: CVE-2021-39327	https://plugi ns.trac.word press.org/ch angeset?sfp_ email=&sfph _mail=&repo name=&old= 2591118%4 0bulletproof- security≠ w=2591118 %40bulletpr oof- security&sfp _email=&sfp h_mail=	A-AIT-BULL- 061021/18
alojapro					
alojapro_widg	get				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The Alojapro Widget WordPress plugin through 1.1.15 doesn't properly sanitise its Custom CSS settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed CVE ID: CVE-2021-24530	N/A	A-ALO-ALOJ- 061021/19
Amazon					
aws_workspa	ces				
Improper	22-Sep-21	9.3	In the Amazon AWS	https://docs.	A-AMA-AWS

Weakness	Publish Date	CVSS	Description	n & CVE	ID	Pa	tch	NCI	PC ID
n of Argument Delimiters in a Command ('Argument Injection')			through 3.1.8 o argument inject workspaces://can lead to remexecution because Chromium Embersamework (Chauncher arguments) fixed in 3.1.9.	tion in t URI har ote cod use of th oedded EF)gp nent. Th	the ndler e ne u- is is	aces/la sergui- azon- works windo client.l windo	ws- html#	06102	1/20
ansi-regex_pr	oject								
ansi-regex									
N/A	17-Sep-21	7.8	ansi-regex is vu Inefficient Regu Expression Con <b>CVE ID : CVE-2</b>	ılar nplexity	7	b.com, /ansi- regex/ it/8d1 58626 4bdc1 d0c58 9, https:/ r.dev/	/comm d7cdb 9882c b7325 c8f76f //hunt bounti 3cf33b 4398-	A-ANS 06102	-ANSI- 1/21
Apache									
druid									
Exposure of Resource to Wrong Sphere	24-Sep-21	4	In the Druid ingestion system, the InputSource is used for reading data from a certain data source. However, the HTTP InputSource allows authenticated users to read data from other sources than intended, such as the local file system, with the privileges of			hread. c9400 ec5cdl 6fc5dc 82961	e.org/t html/r a70d0 b8a348 lb0b52 c0b63 bfbcb9	A-APA 06102	-DRUI- 1/22
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Druid server process. This is not an elevation of privilege when users access Druid directly, since Druid also provides the Local InputSource, which allows the same level of access. But it is problematic when users interact with Druid indirectly through an application that allows users to specify the HTTP InputSource, but not the Local InputSource. In this case, users could bypass the application-level restriction by passing a file URL to the HTTP InputSource. This issue was previously mentioned as being fixed in 0.21.0 as per CVE-2021-26920 but was not fixed in 0.21.0 or 0.21.1.  CVE ID: CVE-2021-36749	dev.druid.ap ache.org%3E , https://lists. apache.org/t hread.html/r 304dfe56a5d fe1b2d9166b 24d2c74ad1 c6730338b2 0aef77a00ed 2be@%3Can nounce.apac he.org%3E	
http_server					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-21	7.5	ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.  CVE ID: CVE-2021-39275	https://http d.apache.org /security/vul nerabilities_ 24.html, https://lists. apache.org/t hread.html/r 82c077663f9 759c7df5a66 56f925b3ee4 f55fcd33c88 9ba7cd6870 29@%3Cuse rs.httpd.apac he.org%3E	A-APA-HTTP- 061021/23

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	16-Sep-21	7.5	A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.  CVE ID: CVE-2021-40438	https://http d.apache.org /security/vul nerabilities_ 24.html, https://lists. apache.org/t hread.html/r 82c077663f9 759c7df5a66 56f925b3ee4 f55fcd33c88 9ba7cd6870 29@%3Cuse rs.httpd.apac he.org%3E	A-APA-HTTP- 061021/24
NULL Pointer Dereference	16-Sep-21	5	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.  CVE ID: CVE-2021-34798	http://httpd. apache.org/s ecurity/vuln erabilities_2 4.html, https://lists. apache.org/t hread.html/r 82c077663f9 759c7df5a66 56f925b3ee4 f55fcd33c88 9ba7cd6870 29@%3Cuse rs.httpd.apac he.org%3E	A-APA-HTTP- 061021/25
Out-of- bounds Read	16-Sep-21	5	A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).	http://httpd. apache.org/s ecurity/vuln erabilities_2 4.html, https://lists. apache.org/t hread.html/r	A-APA-HTTP- 061021/26
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 10 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Desc	cription	1 & CVE	ID	Pa	tch	NCI	IPC ID
jena			CVE ID : 0	CVE-2	021-30	6160		d170ff ab552 8d2ba 17ded @%3C pd.apa		
јена			I				1,			
Improper Restriction of XML External Entity Reference	16-Sep-21	5	A vulnera processin versions allow an a XML Exte including contents or remote secure and the contents of the c	ng in A up to 4 attack ernal E g expos of loca erver.	pache ] 4.1.0, m er to ex ntities sing the al files t	lena, in hay kecute (XXE),	f44d52 f1d009 3f576a 727e1 610d3 93d%4 users.j ache.o , https://apache hread.f44d52 f1d009 3f576a 727e1 610d3	e.org/t html/r 29c54e 97e81 a0823a 669a9f 221d4 40%3C ena.ap rg%3E //lists. e.org/t html/r 29c54e 97e81 a0823a 669a9f 221d4 %3Can e.apac	A-APA 06102	A-JENA- 21/27
kafka										
Observable Discrepancy	22-Sep-21	4.3	Some components in Apache Kafka use `Arrays.equals` to validate a password or key, which is vulnerable to timing attacks that make brute force attacks for such credentials more likely to be successful.				https:/ a.apacl /cve-li	he.org	A-APA 06102	A-KAFK- 21/28
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Users should upgrade to 2.8.1 or higher, or 3.0.0 or higher where this vulnerability has been fixed. The affected versions include Apache Kafka 2.0.0, 2.0.1, 2.1.0, 2.1.1, 2.2.0, 2.2.1, 2.2.2, 2.3.0, 2.3.1, 2.4.0, 2.4.1, 2.5.0, 2.5.1, 2.6.0, 2.6.1, 2.6.2, 2.7.0, 2.7.1, and 2.8.0.  CVE ID: CVE-2021-38153		
shiro					
Improper Authenticati on	17-Sep-21	7.5	Apache Shiro before 1.8.0, when using Apache Shiro with Spring Boot, a specially crafted HTTP request may cause an authentication bypass. Users should update to Apache Shiro 1.8.0.  CVE ID: CVE-2021-41303	https://lists. apache.org/t hread.html/r e470be1ffea 44bca28ccb0 e67a4cf5d74 4e2d2b981d 00fdbbf5abc 13%40%3Ca nnounce.shir o.apache.org %3E	A-APA-SHIR- 061021/29
tomcat					
Improper Input Validation	16-Sep-21	4.3	Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.  CVE ID: CVE-2021-41079	https://lists. apache.org/t hread.html/r ccdef0349fdf 4fb73a4e440 3095446d7f e6264e0a58 e2df5c67994 34%40%3Ca nnounce.tom cat.apache.or g%3E	A-APA-TOMC- 061021/30

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
19-Sep-21	5	All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfo from a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.  CVE ID: CVE-2021-40690	https://lists. apache.org/t hread.html/r 8848751b6a 5dd78cc9e9 9d627e74fec faffdfa1bb61 5dce827aad 633%40%3C dev.santuari o.apache.org %3E, https://lists. apache.org/t hread.html/r bdac116aef9 12b563da54 f4c152222c0 754e32fb2f7 85519ac5e0 59f@%3Cco mmits.tomee .apache.org% 3E	A-APA-TOME- 061021/31
_for_java				
19-Sep-21	5	All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfo from a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.	https://lists. apache.org/t hread.html/r 8848751b6a 5dd78cc9e9 9d627e74fec faffdfa1bb61 5dce827aad 633%40%3C dev.santuari o.apache.org %3E, https://lists. apache.org/t	A-APA-XML 061021/32
	19-Sep-21	19-Sep-21 5	All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.  CVE ID : CVE-2021-40690   All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a	All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfo from a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.  CVE ID : CVE-2021-40690  All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.  All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.  https://lists. apache.org/t hread.html/r bdac116aef9 12b563da54 f4c:152222c0 754e32fb2f7 85519ac5e0 59f@%3Cco mmits.tomee .apache.org/t hread.html/r 8848751b6a 5dd78cc9e9 9d627e74fec faffdfa1bb61 5dce827aad 633%40%3C dev.santuari o.apache.org/t hread.html/r 8848751b6a 5dd78c292 9d627e74fec faffdfa1bb61 5dce827aad 633%40%3C dev.santuari o.apache.org/t hread.html/r 8848751b6a 5dd78c292 9d627e74fec faffdfa1bb61 5dce827aad 633%40%3C dev.santuari o.apache.org/t hread.html/r

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40690	hread.html/r bdac116aef9 12b563da54 f4c152222c0 754e32fb2f7 85519ac5e0 59f@%3Cco mmits.tomee .apache.org% 3E	
Asus					
armoury_crat	e_lite_servic	e			
Uncontrolled Search Path Element	27-Sep-21	4.4	ASUS ROG Armoury Crate Lite before 4.2.10 allows local users to gain privileges by placing a Trojan horse file in the publicly writable %PROGRAMDATA%\ASUS\G amingCenterLib directory.  CVE ID: CVE-2021-40981	N/A	A-ASU-ARMO- 061021/33
Atlassian					
data_center					
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	16-Sep-21	6.5	Affected versions of Atlassian Jira Server or Data Center using the Jira Service Management addon allow remote attackers with JIRA Administrators access to execute arbitrary Java code via a server-side template injection vulnerability in the Email Template feature. The affected versions of Jira Server or Data Center are before version 8.13.12, and from version 8.14.0 before 8.19.1.  CVE ID: CVE-2021-39128	N/A	A-ATL-DATA- 061021/34

1-2

0-1

CVSS Scoring Scale

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
jira							
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	16-Sep-21	6.5	Affected versions of Atlassian Jira Server or Data Center using the Jira Service Management addon allow remote attackers with JIRA Administrators access to execute arbitrary Java code via a server-side template injection vulnerability in the Email Template feature. The affected versions of Jira Server or Data Center are before version 8.13.12, and from version 8.14.0 before 8.19.1.	N/A	A-ATL-JIRA- 061021/35		
avova			CVE ID : CVE-2021-39128				
aveva							
suitelink				I -			
Heap-based Buffer Overflow	23-Sep-21	7.5	Heap-based buffer overflow in SuiteLink server while processing commands $0x05/0x06$ CVE ID : CVE-2021-32959	https://ww w.aveva.com /content/da m/aveva/do cuments/sup port/cyber- security- updates/Sec urityBulletin _AVEVA- 2021- 003.pdf	A-AVE-SUIT- 061021/36		
NULL Pointer Dereference	23-Sep-21	5	Null pointer dereference in SuiteLink server while processing commands $0x03/0x10$ CVE ID : CVE-2021-32963	https://ww w.aveva.com /content/da m/aveva/do cuments/sup port/cyber- security- updates/Sec	A-AVE-SUIT- 061021/37		
updates/Sec							

				urityBulletin _AVEVA- 2021- 003.pdf	
NULL Pointer Dereference	23-Sep-21	5	Null pointer dereference in SuiteLink server while processing command 0x07 CVE ID: CVE-2021-32971	https://ww w.aveva.com /content/da m/aveva/do cuments/sup port/cyber- security- updates/Sec urityBulletin _AVEVA- 2021- 003.pdf	A-AVE-SUIT- 061021/38
NULL Pointer Dereference	23-Sep-21	5	Null pointer dereference in SuiteLink server while processing commands $0x04/0x0a$ CVE ID : CVE-2021-32979	https://ww w.aveva.com /content/da m/aveva/do cuments/sup port/cyber- security- updates/Sec urityBulletin _AVEVA- 2021- 003.pdf	A-AVE-SUIT- 061021/39
NULL Pointer Dereference	23-Sep-21	5	Null pointer dereference in SuiteLink server while processing command 0x0b  CVE ID: CVE-2021-32987	https://ww w.aveva.com /content/da m/aveva/do cuments/sup port/cyber- security- updates/Sec urityBulletin _AVEVA- 2021- 003.pdf	A-AVE-SUIT- 061021/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
Improper Handling of Exceptional Conditions	23-Sep-21	5	Improper handling of exceptional conditions in SuiteLink server while processing command 0x01 CVE ID: CVE-2021-32999	https://ww w.aveva.com /content/da m/aveva/do cuments/sup port/cyber- security- updates/Sec urityBulletin _AVEVA- 2021- 003.pdf	A-AVE-SUIT- 061021/41		
axiosys							
bento4							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-21	6.8	An issue was discovered in Bento4 through v1.6.0-637. A global-buffer-overflow exists in the function AP4_MemoryByteStream::Wr itePartial() located in Ap4ByteStream.cpp. It allows an attacker to cause code execution or information disclosure.  CVE ID: CVE-2021-32265	N/A	A-AXI-BENT- 061021/42		
Baidu							
ueditor							
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-21	3.5	Cross Site Scripting (XSS) vulnerability exists in UEditor v1.4.3.3, which can be exploited by an attacker to obtain user cookie information.  CVE ID: CVE-2021-37271	N/A	A-BAI-UEDI- 061021/43		
zrender							
Improperly Controlled	17-Sep-21	7.5	ZRender is a lightweight graphic library providing 2d	https://githu b.com/ecomf	A-BAI-ZREN- 061021/44		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Modification of Dynamically- Determined Object Attributes			draw for Apache ECharts. In versions prior to 5.2.1, using 'merge' and 'clone' helper methods in the 'src/core/util.ts' module results in prototype pollution. It affects the popular data visualization library Apache ECharts, which uses and exports these two methods directly. The GitHub Security Advisory page for this vulnerability contains a proof of concept. This issue is patched in ZRender version 5.2.1. One workaround is available: Check if there is '_proto_' in the object keys. Omit it before using it as an parameter in these affected methods. Or in 'echarts.util.merge' and 'setOption' if project is using ECharts.  CVE ID: CVE-2021-39227	e/zrender/se curity/advis ories/GHSA- fhv8-fx5f- 7fxf, https://githu b.com/ecomf e/zrender/p ull/826	
bestiaweb			CVEID I GVE EGET GYEE!		
gseor					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	A pageid GET parameter of the GSEOR – WordPress SEO Plugin WordPress plugin through 1.3 is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.  CVE ID: CVE-2021-24396	N/A	A-BES-GSEO- 061021/45
boostnote					
boostnote					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	17-Sep-21	7.5	static/main-preload.js in Boost Note through 0.22.0 allows remote command execution. A remote attacker may send a crafted IPC message to the exposed vulnerable ipcRenderer IPC interface, which invokes the dangerous openExternal Electron API.  CVE ID: CVE-2021-41392	N/A	A-B00-B00S- 061021/46
bootstrapped					
visual_link_pi	review				
Improper Access Control	20-Sep-21	5.5	The Visual Link Preview WordPress plugin before 2.2.3 does not enforce authorisation on several AJAX actions and has the CSRF nonce displayed for all authenticated users, allowing any authenticated user (such as subscriber) to call them and 1) Get and search through title and content of Draft post, 2) Get title of a password-protected post as well as 3) Upload an image from an URL  CVE ID: CVE-2021-24635	N/A	A-B00-VISU- 061021/47
btcpayserver					
btcpay_serve	r				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	26-Sep-21	3.5	btcpayserver is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')  CVE ID: CVE-2021-3830	https://hunt r.dev/bounti es/0fcdee5f- 1f07-47ce- b650- ea8b4a7d35 d8,	A-BTC-BTCP- 061021/48

1-2

0-1

CVSS Scoring Scale

5-6

6-7

8-9

9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Scripting')  butter_project	•			https://githu b.com/btcpa yserver/btcp ayserver/co mmit/fc4e47 cec608cc3db a24b19d014 5ac69320b9 75e	
butter					
N/A	21-Sep-21	5	Butter is a system usability utility. Due to a kernel error the JPNS kernel is being discontinued. Affected users are recommend to update to the Trinity kernel. There are no workarounds.  CVE ID: CVE-2021-39230	https://githu b.com/Frank Enderman/B utter/commi t/a4fd717e8 48306f04f28 23ea5f617e4 da9f5bbdb, https://githu b.com/Frank Enderman/B utter/securit y/advisories /GHSA- 4538-4g86- xf6j	A-BUT-BUTT- 061021/49
bytecodeallia	nce				
wasmtime					
Use After Free	17-Sep-21	3.3	Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing `externref's from the host to guest Wasm content. To trigger the bug, you have to explicitly pass multiple	https://githu b.com/bytec odealliance/ wasmtime/s ecurity/advis ories/GHSA- v4cp-h94r- m7xf	A-BYT- WASM- 061021/50
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			`externref`s from the host to a		
			Wasm instance at the same		
			time, either by passing		
			multiple `externref`s as		
			arguments from host code to		
			a Wasm function, or		
			returning multiple		
			`externref`s to Wasm from a		
			multi-value return function		
			defined in the host. If you do		
			not have host code that		
			matches one of these shapes,		
			then you are not impacted. If		
			Wasmtime's		
			`VMExternRefActivationsTabl		
			e` became filled to capacity		
			after passing the first		
			`externref` in, then passing in		
			the second `externref` could		
			trigger a garbage collection.		
			However the first `externref`		
			is not rooted until we pass		
			control to Wasm, and		
			therefore could be reclaimed		
			by the collector if nothing		
			else was holding a reference		
			to it or otherwise keeping it		
			alive. Then, when control was		
			passed to Wasm after the		
			garbage collection, Wasm		
			could use the first `externref`,		
			which at this point has		
			already been freed. We have		
			reason to believe that the		
			effective impact of this bug is		
			relatively small because		
			usage of `externref` is		
			currently quite rare. The bug		
			has been fixed, and users		
			should upgrade to Wasmtime		
			0.30.0. If you cannot upgrade		

6-7

7-8

8-9

2-3 3-4 4-5

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Wasmtime yet, you can avoid the bug by disabling reference types support in Wasmtime by passing `false` to `wasmtime::Config::wasm_ref erence_types`.		
Out-of- bounds Read	17-Sep-21	3.3	CVE ID: CVE-2021-39216  Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.26.0 and before version 0.30.0 is affected by a memory unsoundness vulnerability. There was an invalid free and out-of-bounds read and write bug when running Wasm that uses 'externref's in Wasmtime. To trigger this bug, Wasmtime needs to be running Wasm that uses 'externref's, the host creates non-null 'externrefs', Wasmtime performs a garbage collection (GC), and there has to be a Wasm frame on the stack that is at a GC safepoint where there are no live references at this safepoint, and there is a safepoint with live references earlier in this frame's function. Under this scenario,	https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-4873-36h9-wv49,https://github.com/bytecodealliance/wasmtime/commit/398a73f0dd862dbe703212ebae8e34036a18c11c	A-BYT- WASM- 061021/51
			Wasmtime would incorrectly use the GC stack map for the safepoint from earlier in the function instead of the empty safepoint. This would result in Wasmtime treating		

5-6

6-7

8-9

7-8

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			arbitrary stack slots as		
			`externref`s that needed to be		
			rooted for GC. At the *next*		
			GC, it would be determined		
			that nothing was referencing		
			these bogus `externref`s		
			(because nothing could ever		
			reference them, because they		
			are not really `externref`s)		
			and then Wasmtime would		
			deallocate them and run		
			` <externref as="" drop="">::drop`</externref>		
			on them. This results in a free		
			of memory that is not		
			necessarily on the heap (and		
			shouldn't be freed at this		
			moment even if it was), as		
			well as potential out-of-		
			bounds reads and writes.		
			Even though support for		
			`externref`s (via the reference		
			types proposal) is enabled by		
			default, unless you are		
			creating non-null `externref`s		
			in your host code or explicitly		
			triggering GCs, you cannot be		
			affected by this bug. We have		
			reason to believe that the		
			effective impact of this bug is		
			relatively small because		
			usage of `externref` is		
			currently quite rare. This bug		
			has been patched and users		
			should upgrade to Wasmtime		
			version 0.30.0. If you cannot		
			upgrade Wasmtime at this		
			time, you can avoid this bug		
			by disabling the reference		
			types proposal by passing		
			`false` to		
			`wasmtime::Config::wasm_ref		
			wasintinecomigwasin_lel		

6-7

7-8

8-9

2-3 3-4 4-5

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			erence_types`.		
			CVE ID : CVE-2021-39218		
Access of Resource Using Incompatible Type ('Type Confusion')	17-Sep-21	3.3	Wasmtime is an open source runtime for WebAssembly & WASI. Wasmtime before version 0.30.0 is affected by a type confusion vulnerability. As a Rust library the 'wasmtime' crate clearly marks which functions are safe and which are 'unsafe', guaranteeing that if consumers never use 'unsafe' then it should not be possible to have memory unsafety issues in their embeddings of Wasmtime. An issue was discovered in the safe API of 'Linker::func_*' APIs. These APIs were previously not sound when one 'Engine' was used to create the 'Linker' and then a different 'Engine' was used to create a 'Store' and then the 'Linker' was used to instantiate a module into that 'Store'. Cross-'Engine' usage of functions is not supported in Wasmtime and this can result in type confusion of function pointers, resulting in being able to safely call a function with the wrong type.  Triggering this bug requires using at least two 'Engine' values in an embedding and then additionally using two different values with a 'Linker' (one at the creation	https://github.com/bytecodealliance/wasmtime/commit/b39f087414f27ae40c44449ed5d1154e03449bff,https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-q879-9g95-56mx	A-BYT- WASM- 061021/52

6-7

8-9

7-8

2-3 3-4 4-5

1-2

0-1

embedded_wireless_controller	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
module with the 'Linker'). It's expected that usage of more- than-one 'Engine' in an embedding is relatively rare since an 'Engine' is intended to be a globally shared resource, so the expectation is that the impact of this issue is relatively small. The fix implemented is to change this behavior to 'paniel()' in Rust instead of silently allowing it. Using different 'Engine' instances with a 'Linker' is a programmer bug that 'wasmtime' catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.3.00. If you cannot upgrade Wasmtime and are using more than one 'Engine' in your embedding it's recommended to instead use only one 'Engine' for the entire program if possible. An 'Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that 'Linker' is only used with one 'Engine'. CVE ID: CVE-2021-39219				time of the `Linker` and			
expected that usage of more- than-one 'Engine' in an embedding is relatively rare since an 'Engine' is intended to be a globally shared resource, so the expectation is that the impact of this issue is relatively small. The fix implemented is to change this behavior to 'panict()' in Rust instead of silently allowing it. Using different' Engine' instances with a 'Linker' is a programmer bug that 'wasmtime' catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.3.0.0. If you cannot upgrade Wasmtime and are using more than one 'Engine' in your embedding it's recommended to instead use only one 'Engine' for the entire program if possible. An 'Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that 'Linker' is only used with one 'Engine'.  CVE ID: CVE-2021-39219				another when instantiating a			
than-one 'Engine' in an embedding is relatively rare since an 'Engine' is intended to be a globally shared resource, so the expectation is that the impact of this issue is relatively small. The fix implemented is to change this behavior to 'panie!()' in Rust instead of silently allowing it. Using different 'Engine' instances with a 'Linker' is a programmer bug that 'wasmtime' catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one 'Engine' in your embedding it's recommended to instead use only one 'Engine' for the entire program if possible. An 'Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that 'Linker' is only used with one 'Engine'.  CVE ID: CVE-2021-39219				module with the `Linker`). It's			
embedding is relatively rare since an 'Engine' is intended to be a globally shared resource, so the expectation is that the impact of this issue is relatively small. The fix implemented is to change this behavior to 'panic!()' in Rust instead of silently allowing it. Using different 'Engine' instances with a 'Linker' is a programmer bug that 'wasmtime' catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one 'Engine' in your embedding it's recommended to instead use only one 'Engine' for the entire program if possible. An 'Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that 'Linker' is only used with one 'Engine'.  CVE ID: CVE-2021-39219				expected that usage of more-			
since an `Engine` is intended to be a globally shared resource, so the expectation is that the impact of this issue is relatively small. The fix implemented is to change this behavior to `panic!()` in Rust instead of silently allowing it. Using different `Engine` instances with a `Linker` is a programmer bug that `wasmtime` catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219				than-one `Engine` in an			
to be a globally shared resource, so the expectation is that the impact of this issue is relatively small. The fix implemented is to change this behavior to `panic!()` in Rust instead of silently allowing it. Using different `Engine' instances with a `Linker' is a programmer bug that `wasmtime' catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine' in your embedding it's recommended to instead use only one `Engine' for the entire program if possible. An `Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine's is required then code should be audited to ensure that `Linker' is only used with one `Engine'.  CVE ID: CVE-2021-39219				embedding is relatively rare			
resource, so the expectation is that the impact of this issue is relatively small. The fix implemented is to change this behavior to 'panic!()' in Rust instead of silently allowing it.  Using different 'Engine' instances with a 'Linker' is a programmer bug that 'wasmtime' catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade to Wasmtime and are using more than one 'Engine' in your embedding it's recommended to instead use only one 'Engine' for the entire program if possible. An 'Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that 'Linker' is only used with one 'Engine'.  CVE ID: CVE-2021-39219				since an `Engine` is intended			
is that the impact of this issue is relatively small. The fix implemented is to change this behavior to 'panic!()' in Rust instead of silently allowing it.  Using different 'Engine' instances with a 'Linker' is a programmer bug that 'wasmtime' catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one 'Engine' in your embedding it's recommended to instead use only one 'Engine' for the entire program if possible. An 'Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that 'Linker' is only used with one 'Engine'.  CVE ID: CVE-2021-39219				to be a globally shared			
is relatively small. The fix implemented is to change this behavior to 'panie!()' in Rust instead of silently allowing it. Using different 'Engine' instances with a 'Linker' is a programmer bug that 'wasmtime' catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one 'Engine' in your embedding it's recommended to instead use only one 'Engine' for the entire program if possible. An 'Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that 'Linker' is only used with one 'Engine'.  CVE ID: CVE-2021-39219				resource, so the expectation			
implemented is to change this behavior to `panic!()` in Rust instead of silently allowing it.  Using different `Engine` instances with a `Linker` is a programmer bug that `wasmtime` catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine' for the entire program if possible. An `Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine's is required then code should be audited to ensure that `Linker' is only used with one `Engine'.  CVE ID: CVE-2021-39219				is that the impact of this issue			
behavior to `panic!()` in Rust instead of silently allowing it.  Using different `Engine` instances with a `Linker` is a programmer bug that `wasmtime` catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219				is relatively small. The fix			
instead of silently allowing it. Using different 'Engine' instances with a 'Linker' is a programmer bug that 'wasmtime' catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one 'Engine' in your embedding it's recommended to instead use only one 'Engine' for the entire program if possible. An 'Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that 'Linker' is only used with one 'Engine'.  CVE ID: CVE-2021-39219				implemented is to change this			
Using different `Engine` instances with a `Linker` is a programmer bug that `wasmtime` catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine' for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine` is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219				behavior to `panic!()` in Rust			
instances with a `Linker` is a programmer bug that `wasmtime` catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219				instead of silently allowing it.			
programmer bug that 'wasmtime' catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one 'Engine' in your embedding it's recommended to instead use only one 'Engine' for the entire program if possible. An 'Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that 'Linker' is only used with one 'Engine'.  CVE ID : CVE-2021-39219				Using different `Engine`			
`wasmtime` catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An 'Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219				instances with a `Linker` is a			
runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine` is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219				programmer bug that			
patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219				`wasmtime` catches at			
upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219				runtime. This bug has been			
version 0.30.0. If you cannot upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219				patched and users should			
upgrade Wasmtime and are using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219				upgrade to Wasmtime			
using more than one `Engine` in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219  Cisco embedded_wireless_controller				•			
in your embedding it's recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219  Cisco  Embedded_wireless_controller							
recommended to instead use only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219  Cisco  embedded_wireless_controller				using more than one `Engine`			
only one `Engine` for the entire program if possible. An `Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219  Cisco  Embedded_wireless_controller							
entire program if possible. An  'Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that 'Linker' is only used with one 'Engine'.  CVE ID: CVE-2021-39219  Cisco  Embedded_wireless_controller				recommended to instead use			
`Engine` is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219  Cisco  Embedded_wireless_controller				, c			
globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219  Cisco embedded_wireless_controller							
is suitable to have only one for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219  Cisco  Embedded_wireless_controller							
for the lifetime of an entire process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219  Cisco  embedded_wireless_controller							
process. If using multiple `Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID : CVE-2021-39219  Cisco embedded_wireless_controller				•			
`Engine`s is required then code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID: CVE-2021-39219  Cisco  embedded_wireless_controller							
code should be audited to ensure that `Linker` is only used with one `Engine`.  CVE ID : CVE-2021-39219  Cisco embedded_wireless_controller							
ensure that `Linker` is only used with one `Engine`.  CVE ID : CVE-2021-39219  Cisco  embedded_wireless_controller				_			
used with one `Engine`.  CVE ID : CVE-2021-39219  Embedded_wireless_controller							
Cisco embedded_wireless_controller							
Cisco embedded_wireless_controller				used with one `Engine`.			
embedded_wireless_controller				CVE ID : CVE-2021-39219			
	Cisco						
	embedded_w	embedded_wireless_controller					
CVSS Scoring Scale	CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP.  CVE ID: CVE-2021-1615	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-iosxe-ewc-dosg6JruHRT	A-CIS-EMBE- 061021/53
ios_xe					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cbr8- cops- Vc2ZsJSx	A-CIS-IOS 061021/54

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  CVE ID: CVE-2021-1622		
sd-wan					
Insufficiently Protected Credentials	23-Sep-21	3.5	A vulnerability in the disaster recovery feature of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to gain unauthorized access to user credentials. This vulnerability exists because access to API endpoints is not properly restricted. An attacker could exploit this vulnerability by sending a request to an API endpoint. A successful exploit could allow the attacker to gain unauthorized access to administrative credentials that could be used in further attacks.  CVE ID: CVE-2021-1589	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- credentials- ydYfskzZ	A-CIS-SD-W- 061021/55
Improper Link Resolution Before File Access ('Link Following')	23-Sep-21	6.6	A vulnerability in the Cisco IOS XE SD-WAN Software CLI could allow an authenticated, local attacker to overwrite arbitrary files on the local system. This vulnerability is due to improper access controls on files within the	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- GjR5pG0m	A-CIS-SD-W- 061021/56

1-2

0-1

5-6

6-7

8-9

9-10

7-8

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system. A successful exploit could allow the attacker to overwrite arbitrary files on an affected device.  CVE ID: CVE-2021-1612		
sd-wan_vbone	d_orchestrate	or			
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX	A-CIS-SD-W- 061021/57
sd-wan_vman	age				
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX	A-CIS-SD-W- 061021/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by running a CI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546		
wireless_lan_e	controller_sc	oftware	:		
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privilege equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	A-CIS-WIRE- 061021/59
client					
jointjs					
Access of Resource Using	21-Sep-21	7.5	This affects the package jointjs before 3.4.2. A type confusion vulnerability can	https://snyk. io/vuln/SNY K-JAVA-	A-CLI-JOIN- 061021/60
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Descript	on & CVE	ID	Pat	tch	NCI	IPC ID
Incompatible Type ('Type Confusion')			lead to a bypa 28480 when a provided key path paramet the setByPath CVE ID : CVE	the user- s used in er are ar i function	the rays in 1.	ORGWI SBOWI 16558: https://b.com/ O/joint ses/tag 2, https://io/vuln K-JS- JOINTJ 15795: https://io/vuln K-JAVA ORGWI SNPM- 16558: https://b.com/ O/joint 1514	ER- 17, /githu /clientI t/relea g/v3.4. /snyk. n/SNY S- 78, /snyk. n/SNY L- EBJAR 16, /githu /clientI		
cloudron									
cloudron									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-21	4.3	In Cloudron 6 parameter on is vulnerable XSS.  CVE ID : CVE	the login to Reflec	n page ted	N/A		A-CLO 06102	-CLOU- 1/61
coder									
code-server									
N/A	17-Sep-21	7.8	code-server is Inefficient Re Expression Co	gular		https:// r.dev/b es/388 3-30fc-	oounti 88851	A-COE 06102	0-CODE- 1/62
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-3810	805d- 34070d60e2 23, https://githu b.com/cdr/c ode- server/com mit/ca617df 135e78833f 93c8320cb2 d2cf8bba809 f5	
concretecms					
concrete_cms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Sep-21	6.5	An issue was discovered in Concrete CMS through 8.5.5. Authenticated path traversal leads to to remote code execution via uploaded PHP code, related to the bFilename parameter.  CVE ID: CVE-2021-40097	https://docu mentation.co ncretecms.or g/developers /introductio n/version- history/856- release-notes	A-CON-CONC- 061021/63
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Sep-21	7.5	An issue was discovered in Concrete CMS through 8.5.5. Path Traversal leading to RCE via external form by adding a regular expression.  CVE ID: CVE-2021-40098	https://docu mentation.co ncretecms.or g/developers /introductio n/version- history/856- release-notes	A-CON-CONC- 061021/64
N/A	24-Sep-21	6.5	An issue was discovered in Concrete CMS through 8.5.5. Fetching the update json scheme over HTTP leads to remote code execution.  CVE ID: CVE-2021-40099	https://docu mentation.co ncretecms.or g/developers /introductio n/version- history/856- release-notes	A-CON-CONC- 061021/65

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	24-Sep-21	3.5	An issue was discovered in Concrete CMS through 8.5.5. Stored XSS can occur in Conversations when the Active Conversation Editor is set to Rich Text.  CVE ID: CVE-2021-40100	https://docu mentation.co ncretecms.or g/developers /introductio n/version- history/856- release-notes	A-CON-CONC- 061021/66
Deserializati on of Untrusted Data	24-Sep-21	6.4	An issue was discovered in Concrete CMS through 8.5.5. Arbitrary File deletion can occur via PHAR deserialization in is_dir (PHP Object Injection associated with the _wakeup magic method).  CVE ID: CVE-2021-40102	https://docu mentation.co ncretecms.or g/developers /introductio n/version- history/856- release-notes	A-CON-CONC- 061021/67
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Sep-21	5	An issue was discovered in Concrete CMS through 8.5.5. Path Traversal can lead to Arbitrary File Reading and SSRF.  CVE ID: CVE-2021-40103	https://docu mentation.co ncretecms.or g/developers /introductio n/version- history/856- release-notes	A-CON-CONC- 061021/68
Incorrect Authorizatio n	27-Sep-21	5	An issue was discovered in Concrete CMS through 8.5.5. There is an SVG sanitizer bypass.  CVE ID: CVE-2021-40104	https://docu mentation.co ncretecms.or g/developers /introductio n/version- history/856- release-notes	A-CON-CONC- 061021/69
Improper Neutralizatio n of Input During Web Page Generation	27-Sep-21	4.3	An issue was discovered in Concrete CMS through 8.5.5. There is XSS via Markdown Comments.  CVE ID: CVE-2021-40105	https://docu mentation.co ncretecms.or g/developers /introductio n/version-	A-CON-CONC- 061021/70

6-7

8-9

7-8

2-3 3-4 4-5

1-2

0-1

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				history/856- release-notes	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	4.3	An issue was discovered in Concrete CMS through 8.5.5. There is unauthenticated stored XSS in blog comments via the website field.  CVE ID: CVE-2021-40106	https://docu mentation.co ncretecms.or g/developers /introductio n/version- history/856- release-notes	A-CON-CONC- 061021/71
Cross-Site Request Forgery (CSRF)	27-Sep-21	6.8	An issue was discovered in Concrete CMS through 8.5.5. The Calendar is vulnerable to CSRF. ccm_token is not verified on the ccm/calendar/dialogs/event /add/save endpoint.  CVE ID: CVE-2021-40108	https://docu mentation.co ncretecms.or g/developers /introductio n/version- history/856- release-notes	A-CON-CONC- 061021/72
Server-Side Request Forgery (SSRF)	27-Sep-21	5.5	A SSRF issue was discovered in Concrete CMS through 8.5.5. Users can access forbidden files on their local network. A user with permissions to upload files from external sites can upload a URL that redirects to an internal resource of any file type. The redirect is followed and loads the contents of the file from the redirected-to server. Files of disallowed types can be uploaded.  CVE ID: CVE-2021-40109	https://docu mentation.co ncretecms.or g/developers /introductio n/version- history/856- release-notes	A-CON-CONC- 061021/73
Cross-Site Request Forgery (CSRF)	23-Sep-21	5.8	A CSRF in Concrete CMS version 8.5.5 and below allows an attacker to duplicate files which can lead to UI inconvenience, and	N/A	A-CON-CONC- 061021/74

6-7

8-9

7-8

2-3 3-4 4-5

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			exhaustion of disk space.Credit for discovery: "Solar Security CMS Research Team"		
			CVE ID : CVE-2021-22949		
Cross-Site Request Forgery (CSRF)	23-Sep-21	4.3	Concrete CMS prior to 8.5.6 had a CSFR vulnerability allowing attachments to comments in the conversation section to be deleted.Credit for discovery: "Solar Security Research Team"	N/A	A-CON-CONC- 061021/75
			CVE ID : CVE-2021-22950		
Cross-Site Request Forgery (CSRF)	23-Sep-21	5.8	A CSRF in Concrete CMS version 8.5.5 and below allows an attacker to clone topics which can lead to UI inconvenience, and exhaustion of disk space.Credit for discovery: "Solar Security Research Team"  CVE ID: CVE-2021-22953	N/A	A-CON-CONC- 061021/76
cookiex-deep	proiect				
cookiex-deep					
Improperly Controlled Modification of Dynamically- Determined Object Attributes	17-Sep-21	7.5	This affects all versions of package @cookiex/deep. The global proto object can be polluted using the _proto_ object.  CVE ID: CVE-2021-23442	https://githu b.com/tony- tsx/cookiex- deep/issues/ 1, https://snyk. io/vuln/SNY K-JS- COOKIEXDE EP-1582793, https://githu b.com/tony-	A-COO-COOK- 061021/77

1-2

0-1

CVSS Scoring Scale

5-6

6-7

7-8

8-9

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
				tsx/cookiex- deep/commi t/b5bea2b7f 34a5fa9abb4 446cbd038e cdbcd09c88	
couchbase					
couchbase_se	erver				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Sep-21	5	Couchbase Server 6.5.x, 6.6.x through 6.6.2, and 7.0.0 has a Buffer Overflow. A specially crafted network packet sent from an attacker can crash memcached.  CVE ID: CVE-2021-35944	https://ww w.couchbase. com/alerts, https://docs. couchbase.co m/server/cu rrent/releas e- notes/relnot es.html	A-COU-COUC- 061021/78
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Sep-21	5	Couchbase Server 6.5.x, 6.6.0 through 6.6.2, and 7.0.0, has a Buffer Overflow. A specially crafted network packet sent from an attacker can crash memcached.  CVE ID: CVE-2021-35945	https://ww w.couchbase. com/alerts, https://docs. couchbase.co m/server/cu rrent/releas e- notes/relnot es.html	A-COU-COUC- 061021/79
creolabs					
gravity					
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in gravity through 0.8.1. A heap-buffer-overflow exists in the function gnode_function_add_upvalue located in gravity_ast.c. It allows an attacker to cause code Execution.	N/A	A-CRE-GRAV- 061021/80

1-2

0-1

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-32281		
Out-of- bounds Write	20-Sep-21	4.3	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function ircode_add_check() located in gravity_ircode.c. It allows an attacker to cause Denial of Service.	N/A	A-CRE-GRAV- 061021/81
			CVE ID : CVE-2021-32282		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function gravity_string_to_value() located in gravity_value.c. It allows an attacker to cause Denial of Service.	N/A	A-CRE-GRAV- 061021/82
			CVE ID : CVE-2021-32283		
NULL Pointer Dereference	20-Sep-21	6.8	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function ircode_register_pop_context_ protect() located in gravity_ircode.c. It allows an attacker to cause Denial of Service.	N/A	A-CRE-GRAV- 061021/83
			CVE ID : CVE-2021-32284		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in gravity through 0.8.1. A NULL pointer dereference exists in the function list_iterator_next() located in gravity_core.c. It allows an attacker to cause Denial of Service.	N/A	A-CRE-GRAV- 061021/84
			CVE ID : CVE-2021-32285		

5-6

6-7

7-8

8-9

CVSS Scoring Scale

Authenticated Stored Cross-Site Scripting (XSS) vulnerability in WordPress Absolutely Glamorous Custom Admin plugin (versions <= 6.8). Stored XSpage Generation ('Cross-site Scripting')	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
Authenticated Stored Cross- Site Scripting (XSS)   Nulnerability in WordPress   Absolutely Glamorous   Natsolutely Glamorous   Dadge Generation ('Cross-site Scripting')   23-Sep-21   Scripting')   23-Sep-21   3.5	cusmin	usmin								
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')  Dadamailproject  Total Analy  Dadamailproject  Dadamailproject  Dada Mail is a web-based e-mail list management system. In affected versions a bad actor could give someone a carefully crafted web page via email, SMS, etc, that - when visited, allows them control of the list control panel as if the bad actor was logged in themselves. This includes changing any mailing list password - which could effectively shut out actual list owners of the mailing list and allow the bad actor could effectively shut out actual list owners of the mailing list. This vulnerability also affects profile logins. For this vulnerability to work, the target of the bad actor would  Site Scripting (XSS) vulnerability in WordPress Absolutely Glamorous neckson dathout plugin ps.svn.wordp ress.org/ag-custom-admin/trunk //changelog.t A-CUS-ABSO-061021/85  A-CUS-BSO-061021/85  A-CUS-ABSO-061021/85  A-	absolutely_glamorous_custom_admin									
Cross-Site Request Forgery (CSRF)  20-Sep-21  6.8  Dada Mail is a web-based e-mail list management system. In affected versions a bad actor could give someone a carefully crafted web page via email, SMS, etc, that - when visited, allows them control of the list control panel as if the bad actor was logged in themselves. This includes changing any mailing list password, as well as the Dada Mail Root Password - which could effectively shut out actual list owners of the mailing list and allow the bad actor complete and unfettered control of your mailing list. This vulnerability also affects profile logins. For this vulnerability to work, the target of the bad actor would  Dada Mail is a web-based e-mail list aweb-based e-mail list management system. In affected versions a bad actor could give someone a carefully crafted web page via email/commit //d4d3d86d0 8:6816b4da7 5a5ef45abc1 2188772459, https://githu b.com/justin git/dada-mail/securit y/advisories //GHSA-344m-p829-2r38	Neutralizatio n of Input During Web Page Generation ('Cross-site	23-Sep-21	3.5	Site Scripting (XSS) vulnerability in WordPress Absolutely Glamorous Custom Admin plugin (versions <= 6.8). Stored XSS possible via unsanitized input fields of the plugin settings, some of the payloads could make the frontend and the backend inaccessible.	ns.svn.wordp ress.org/ag- custom- admin/trunk /changelog.t					
Cross-Site Request Forgery (CSRF)  Coross-Site Request Forgery (CSRF)  Coross-Site Request Forgery (CSRF)  Request Forgery (CSRF)  Coross-Site Request Possevord Possevo	Dadamailpro	ject								
Cross-Site Request Forgery (CSRF)  6.8  mail list management system. In affected versions a bad actor could give someone a carefully crafted web page via email, SMS, etc, that - when visited, allows them control of the list control panel as if the bad actor was logged in themselves. This includes changing any mailing list password, as well as the Dada Mail Root Password - which could effectively shut out actual list owners of the mailing list and allow the bad actor complete and unfettered control of your mailing list. This vulnerability also affects profile logins. For this vulnerability to work, the target of the bad actor would  milttps://githu b.com/justin git/dada-mail/securit y/advisories /GHSA-344m-p829-2r38	dada_mail									
	Request Forgery	20-Sep-21	6.8	mail list management system. In affected versions a bad actor could give someone a carefully crafted web page via email, SMS, etc, that - when visited, allows them control of the list control panel as if the bad actor was logged in themselves. This includes changing any mailing list password, as well as the Dada Mail Root Password - which could effectively shut out actual list owners of the mailing list and allow the bad actor complete and unfettered control of your mailing list. This vulnerability also affects profile logins. For this vulnerability to work, the target of the bad actor would	b.com/justin git/dada-mail/commit /d4d3d86d0 8c816b4da7 5a5ef45abc1 2188772459, https://github.com/justin git/dada-mail/securit y/advisories /GHSA-344m-p829-	DADA-				

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pa	itch	NCI	IPC ID
			This CS Dada Mof Dada below. no kno have he this vu confirm by a th advised 11.16.0	SRF vultail affe a Mail vertical Althous own CSR appeneer linerabilities and to upon the control of the control	themselinerability cts all von 11.15.1 gh we know the lity has library. Users late to von 12021-4	ersions and now of its that wild, been ng, and are ersion				
Datev										
framework_li	brary									
Incorrect Permission Assignment for Critical Resource	23-Sep-21	7.5	Update 5.8.0.2 12.5.10 progra attacke via inst of serv	12.5.1001.5 in DATEV programs v14.1 allows attacker to escalate privileges via insufficient configuration		datev. p- center	//apps. de/hel ·/docu /1021	A-DA7 06102	Γ-FRAM- 21/87	
program										
Incorrect Permission Assignment for Critical Resource	23-Sep-21	7.5	Update 5.8.0.2 12.5.10 progra attacke via inst of serv	Insecure permissions in Update Manager <= 5.8.0.2300 and DFL <= 12.5.1001.5 in DATEV programs v14.1 allows attacker to escalate privileges via insufficient configuration of service components.  CVE ID: CVE-2021-41428		datev.	//apps. de/hel ·/docu /1021	A-DAT 06102	Γ-PROG- 21/88	
update_mana	ger									
Incorrect Permission Assignment	23-Sep-21	7.5	Update	Insecure permissions in Update Manager <= 5.8.0.2300 and DFL <=				//apps. de/hel	A-DAT 06102	T-UPDA- 21/89
CVSS Scoring Sca	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
for Critical Resource			12.5.1001.5 in DATEV programs v14.1 allows attacker to escalate privileges via insufficient configuration of service components.  CVE ID: CVE-2021-41428	center/docu ments/1021 197			
Dell							
emc_network	er						
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-21	4	Dell NetWorker, versions 18.x and 19.x contain a Path traversal vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and gain access to unauthorized information.  CVE ID: CVE-2021-21569	https://ww w.dell.com/s upport/kbdo c/en- us/0001883 11/	A-DEL-EMC 061021/90		
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	28-Sep-21	4	Dell NetWorker, versions 18.x and 19.x contain an Information disclosure vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and gain access to unauthorized information.  CVE ID: CVE-2021-21570	https://ww w.dell.com/s upport/kbdo c/en- us/0001883 11/dsa- 2021-124- dell- networker- security- update-for- multiple- vulnerabilitie s	A-DEL-EMC 061021/91		
supportassist	t_client_consu	umer					
Improper Limitation of a Pathname to a Restricted	28-Sep-21	3.6	Dell SupportAssist Client Consumer versions 3.9.13.0 and any versions prior to 3.9.13.0 contain an arbitrary file deletion vulnerability that	https://ww w.dell.com/s upport/kbdo c/en- us/0001910	A-DEL-SUPP- 061021/92		

6-7

7-8

8-9

2-3 3-4 4-5

1-2

0-1

device42 device42			can be exploited by using the Windows feature of NTFS called Symbolic links.  Symbolic links can be created by any(non-privileged) user under some object directories, but by themselves are not sufficient to successfully escalate privileges. However, combining them with a different object, such as the NTFS junction point allows for the exploitation. Support assist clean files functionality do not distinguish junction points from the physical folder and proceeds to clean the target of the junction that allows nonprivileged users to	57/dsa- 2021-163- dell- supportassis t-client- consumer- security- update-for- two- vulnerabilitie s	
			create junction points and delete arbitrary files on the system which can be accessed only by the admin.  CVE ID: CVE-2021-36286		
device42					
Improper Neutralizatio n of Argument Delimiters in a Command ('Argument Injection')	17-Sep-21	8.5	The Device42 Main Appliance before 17.05.01 does not sanitize user input in its Nmap Discovery utility. An attacker (with permissions to add or edit jobs run by this utility) can inject an extra argument to overwrite arbitrary files as the root user on the Remote Collector.  CVE ID: CVE-2021-41316	https://docs. device42.co m/auto- discovery/n map- autodiscover y/, https://blog. device42.co m/2021/09/ critical-fixes- in-17-05- 01/,	A-DEV-DEVI- 061021/93

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			https://docs. device42.co m/auto- discovery/re mote- collector-rc/				
tor							
17-Sep-21	9	The Device42 Remote Collector before 17.05.01 does not sanitize user input in its SNMP Connectivity utility. This allows an authenticated attacker (with access to the console application) to execute arbitrary OS commands and escalate privileges.  CVE ID: CVE-2021-41315	https://blog. device42.co m/2021/09/ critical-fixes- in-17-05- 01/, https://docs. device42.co m/auto- discovery/re mote- collector-rc/	A-DEV- REMO- 061021/94			
unter							
20-Sep-21	3.5	The Post Views Counter WordPress plugin before 1.3.5 does not sanitise or escape its Post Views Label settings, which could allow high privilege users to perform Cross-Site Scripting attacks in the frontend even when the unfiltered_html capability is disallowed  CVE ID : CVE-2021-24613	N/A	A-DFA-POST- 061021/95			
nroject		CVE ID: CVE-2U21-24013					
display_users_project display_users							
20-Sep-21	6.5	The Edit Role functionality in the Display Users WordPress plugin through 2.0.0 had an 'id' parameter which is not	N/A	A-DIS-DISP- 061021/96			
	ounter  20-Sep-21  _project	17-Sep-21 9  Dunter  20-Sep-21 3.5	The Device42 Remote Collector before 17.05.01 does not sanitize user input in its SNMP Connectivity utility. This allows an authenticated attacker (with access to the console application) to execute arbitrary OS commands and escalate privileges. CVE ID : CVE-2021-41315  The Post Views Counter WordPress plugin before 1.3.5 does not sanitise or escape its Post Views Label settings, which could allow high privilege users to perform Cross-Site Scripting attacks in the frontend even when the unfiltered_html capability is disallowed CVE ID : CVE-2021-24613  _project  The Edit Role functionality in the Display Users WordPress	https://docs. device42.co m/auto-discovery/re mote-collector-rc/  The Device42 Remote Collector before 17.05.01 does not sanitize user input in its SNMP Connectivity utility. This allows an authenticated attacker (with access to the console application) to execute arbitrary OS commands and escalate privileges.  CVE ID : CVE-2021-41315  The Post Views Counter WordPress plugin before 1.3.5 does not sanitise or escape its Post Views Label settings, which could allow high privilege users to perform Cross-Site Scripting attacks in the frontend even when the unfiltered_html capability is disallowed CVE ID : CVE-2021-24613  Purpoject  The Edit Role functionality in the Display Users WordPress N/A			

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.  CVE ID: CVE-2021-24400		
dpl					
product_feed	on_woocom	merce			
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The fetch_product_ajax functionality in the Product Feed on WooCommerce WordPress plugin before 3.3.1.0 uses a `product_id` POST parameter which is not properly sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.  CVE ID: CVE-2021-24511	https://code vigilant.com/ disclosure/2 021/wp- plugin- purple-xmls- google- product- feed-for- woocommer ce/	A-DPL-PROD- 061021/97
Ec-cube					
ec-cube					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-21	4.3	Cross-site scripting vulnerability in List (order management) item change plug-in (for EC-CUBE 3.0 series) Ver.1.1 and earlier allows a remote attacker to inject an arbitrary script via unspecified vectors.  CVE ID: CVE-2021-20825	N/A	A-ECEC-C- 061021/98
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-21	4.3	Cross-site scripting vulnerability in Order Status Batch Change Plug-in (for ECCUBE 3.0 series) all versions allows a remote attacker to inject an arbitrary script via unspecified vectors.  CVE ID: CVE-2021-20828	N/A	A-ECEC-C- 061021/99

1-2

0-1

5-6

6-7

7-8

8-9

9-10

eid_easy  Improper Neutralizatio nof Input During Web Page Generation ('Cross-site Scripting')  elv  elv  elvish  Exposure of Resource to Wrong Sphere  The eID Easy WordPress plugin is vulnerable to Reflected Cross-Site Scripting plugin is vulnerable to the expanding in stracword press. Grapk plugin is vulnerable to the Reflected Cross-Site Scripting plugin is vulnerable to the Reflected Cross-Site Scripting plugin is vulnerable to the expanding in stracword press. Grapk plugin is vulnerable to the expanding in stracword press. Grapk plugin is vulnerable to the expanding in stracword press. Grapk plugin is vulnerable to the expanding in stracword press. Grapk plugin is vulnerable to the expanding in stracword press. Grapk plugin is vulnerable to the expanding in stracword press. Grapk plugin is tracword	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')  20-Sep-21  4.3  Elvish is a programming language and interactive shell, combined into one package. In versions prior to 0.14.0 Elvish's web UI backend (estarted by 'elvish - web') hosts an endpoint that allows executing the code sent from the web UI. The backend does not check the origin of requests correctly. As a result, if the user has the web UI backend open and visits a compromised or malicious website, the web site can send arbitrary code to the endpoint in localhost. All Elvish releases from 0.14.0 onward no longer include the the web UI, although it is still possible for the user to build a version from source that includes the web UI. The issue can be	eideasy								
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')  elv  elv  elv  elvs  Exposure of Resource to Wrong Sphere  Plugin is vulnerable to Reflected Cross-Site Scripting via the error parameter found in the ~/admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 4.6.  CVE ID : CVE-2021-34650  Elvish is a programming language and interactive shell, combined into one package. In versions prior to 0.14.0 Elvish's web UI backend (started by 'elvish - web') hosts an endpoint that allows executing the code sent from the web UI. The backend does not check the origin of requests correctly.  As a result, if the user has the web UI backend open and visits a compromised or malicious website, the website can send arbitrary code to the endpoint in localhost. All Elvish releases from 0.14.0 onward no longer include the the web UI, although it is still possible for the user to build a version from source that includes the web UI. The issue can be	eid_easy								
Exposure of Resource to Wrong Sphere  23-Sep-21  Elvish is a programming language and interactive shell, combined into one package. In versions prior to 0.14.0 Elvish's web UI backend (started by 'elvish-web') hosts an endpoint that allows executing the code sent from the web UI. The backend does not check the origin of requests correctly. As a result, if the user has the web UI backend open and visits a compromised or malicious website, the website can send arbitrary code to the endpoint in localhost. All Elvish releases from 0.14.0 onward no longer include the the web UI, although it is still possible for the user to build a version from source that includes the web UI. The issue can be	Neutralizatio n of Input During Web Page Generation ('Cross-site	20-Sep-21	4.3	plugin is vulnerable to Reflected Cross-Site Scripting via the error parameter found in the ~/admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 4.6.	ns.trac.word press.org/br owser/smart - id/trunk/ad min.php?rev =2451347#L	_			
Exposure of Resource to Wrong Sphere  23-Sep-21  Elvish is a programming language and interactive shell, combined into one package. In versions prior to 0.14.0 Elvish's web UI backend (started by 'elvish - web') hosts an endpoint that allows executing the code sent from the web UI. The backend does not check the origin of requests correctly. As a result, if the user has the web UI backend open and visits a compromised or malicious website, the website can send arbitrary code to the endpoint in localhost. All Elvish releases from 0.14.0 onward no longer include the the web UI, although it is still possible for the user to build a version from source that includes the web UI. The issue can be									
Exposure of Resource to Wrong Sphere  23-Sep-21  23-Sep-21  Exposure of Resource to Wrong Sphere  23-Sep-21  24-Sep-21  24-Sep-21  24-Sep-21  24-Sep-21  24-Sep-21  2	elvish								
	Resource to Wrong	23-Sep-21	9.3	language and interactive shell, combined into one package. In versions prior to 0.14.0 Elvish's web UI backend (started by 'elvish - web') hosts an endpoint that allows executing the code sent from the web UI. The backend does not check the origin of requests correctly. As a result, if the user has the web UI backend open and visits a compromised or malicious website, the website can send arbitrary code to the endpoint in localhost. All Elvish releases from 0.14.0 onward no longer include the the web UI, although it is still possible for the user to build a version from source that includes the web UI. The issue can be	b.com/elves/ elvish/securi ty/advisories /GHSA-fpv6- f8jw-rc3r, https://githu b.com/elves/ elvish/comm it/ccc275003 7bbbfafe9c1 b7a78eadd3				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			by removing the web UI (found in web, pkg/web or pkg/prog/web, depending on the exact version).		
			CVE ID : CVE-2021-41088		
enbra					
ewm					
Use of Hard- coded Credentials	16-Sep-21	2.9	Multiple Wireless M-Bus devices by Enbra use Hard-coded Credentials in Security mode 5 without an option to change the encryption key. An adversary can learn all information that is available in Enbra EWM.  CVE ID: CVE-2021-34571	https://ww w.fit.vutbr.cz /~polcak/CV E-2021- 34571.en	A-ENB-EWM- 061021/102
			Enbra EWM 1.7.29 does not		
Insufficient Verification of Data Authenticity	16-Sep-21	3.3	check for or detect replay attacks sent by wireless M-Bus Security mode 5 devices. Instead timestamps of the sensor are replaced by the time of the readout even if the data is a replay of earlier data.  CVE ID: CVE-2021-34572	https://ww w.fit.vutbr.cz /~polcak/CV E-2021- 34572.en	A-ENB-EWM- 061021/103
			In Enbra EWM in Version		
Incorrect Calculation	16-Sep-21	2.1	1.7.29 together with several tested wireless M-Bus Sensors the events backflow and "no flow" are not reconized or misinterpreted. This may lead to wrong values and missing events.	https://ww w.fit.vutbr.cz /~polcak/CV E-2021- 34573.en	A-ENB-EWM- 061021/104
			CVE ID : CVE-2021-34573		
Ericsson					
enterprise_co	ntent_manag	gement			

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
17-Sep-21	6	In Ericsson ECM before 18.0, it was observed that Security Provider Endpoint in the User Profile Management Section is vulnerable to CSV Injection.  CVE ID: CVE-2021-41390	N/A	A-ERI-ENTE- 061021/105
17-Sep-21	3.5	In Ericsson ECM before 18.0, it was observed that Security Management Endpoint in User Profile Management Section is vulnerable to stored XSS via a name, leading to session hijacking and full account takeover.  CVE ID: CVE-2021-41391	N/A	A-ERI-ENTE- 061021/106
20-Sep-21	6.8	An issue was discovered in faad2 before 2.10.0. A heap-buffer-overflow exists in the function stszin located in mp4read.c. It allows an attacker to cause Code Execution.	https://githu b.com/knik0 /faad2/com mit/1b71a6b a963d13137 5f5e489b3b2 5e36f19f3f2	A-FAA-FAAD- 061021/107
20-Sep-21	6.8	An issue was discovered in faad2 through 2.10.0. A stackbuffer-overflow exists in the function ftypin located in mp4read.c. It allows an attacker to cause Code Execution.  CVE ID: CVE-2021-32273	N/A	A-FAA-FAAD- 061021/108
		CILIDICIE ECET CEE/C		
	17-Sep-21  17-Sep-21  20-Sep-21	17-Sep-21 6  17-Sep-21 3.5  20-Sep-21 6.8	In Ericsson ECM before 18.0, it was observed that Security Provider Endpoint in the User Profile Management Section is vulnerable to CSV Injection.  CVE ID: CVE-2021-41390  In Ericsson ECM before 18.0, it was observed that Security Management Endpoint in User Profile Management Section is vulnerable to stored XSS via a name, leading to session hijacking and full account takeover.  CVE ID: CVE-2021-41391  An issue was discovered in faad2 before 2.10.0. A heap-buffer-overflow exists in the function stszin located in mp4read.c. It allows an attacker to cause Code Execution.  CVE ID: CVE-2021-32272  An issue was discovered in faad2 through 2.10.0. A stack-buffer-overflow exists in the function ftypin located in mp4read.c. It allows an attacker to cause Code	In Ericsson ECM before 18.0, it was observed that Security Provider Endpoint in the User Profile Management Section is vulnerable to CSV Injection.  CVE ID: CVE-2021-41390  In Ericsson ECM before 18.0, it was observed that Security Management Endpoint in User Profile Management Section is vulnerable to stored XSS via a name, leading to session hijacking and full account takeover. CVE ID: CVE-2021-41391  An issue was discovered in faad2 before 2.10.0. A heap-buffer-overflow exists in the function stszin located in mp4read.c. It allows an attacker to cause Code Execution. CVE ID: CVE-2021-32272  An issue was discovered in faad2 through 2.10.0. A stack-buffer-overflow exists in the function ftypin located in mp4read.c. It allows an attacker to cause Code  20-Sep-21  6.8  In Ericsson ECM before 18.0, it was observed in faad2 before 2.10.0. A heap-buffer overflow exists in the function ftypin located in mp4read.c. It allows an attacker to cause Code  8.8  An issue was discovered in faad2 through 2.10.0. A stack-buffer-overflow exists in the function ftypin located in mp4read.c. It allows an attacker to cause Code

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
		buffer-overflow exists in the function sbr_qmf_synthesis_64 located in sbr_qmf.c. It allows an attacker to cause code Execution.					
		CVE ID : CVE-2021-32274					
20-Sep-21	4.3	An issue was discovered in faad2 through 2.10.0. A NULL pointer dereference exists in the function get_sample() located in output.c. It allows an attacker to cause Denial of Service.	N/A	A-FAA-FAAD- 061021/110			
		CVE ID : CVE-2021-32276					
20-Sep-21	6.8	An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function sbr_qmf_analysis_32 located in sbr_qmf.c. It allows an attacker to cause code Execution.	N/A	A-FAA-FAAD- 061021/111			
		CVE ID : CVE-2021-32277					
20-Sep-21	6.8	An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function lt_prediction located in lt_predict.c. It allows an attacker to cause code Execution.	N/A	A-FAA-FAAD- 061021/112			
		CVE ID : CVE-2021-32278					
Ffmpeg  ffmpeg							
20-Sep-21	6.8	Integer Overflow vulnerability in function filter16_roberts in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows	https://git.ff mpeg.org/git web/ffmpeg. git/commit/ 99f8d32129	A-FFM-FFMP- 061021/113			
	20-Sep-21 20-Sep-21	20-Sep-21 4.3 20-Sep-21 6.8	buffer-overflow exists in the function sbr_qmf_synthesis_64 located in sbr_qmf.c. It allows an attacker to cause code Execution.  CVE ID : CVE-2021-32274  An issue was discovered in faad2 through 2.10.0. A NULL pointer dereference exists in the function get_sample() located in output.c. It allows an attacker to cause Denial of Service.  CVE ID : CVE-2021-32276  An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function sbr_qmf_analysis_32 located in sbr_qmf_c. It allows an attacker to cause code Execution.  CVE ID : CVE-2021-32277  An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function lt_prediction located in lt_predict.c. It allows an attacker to cause code Execution.  CVE ID : CVE-2021-32277  An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function lt_prediction located in lt_predict.c. It allows an attacker to cause code Execution.  CVE ID : CVE-2021-32278  Integer Overflow vulnerability in function filter16_roberts in libavfilter/vf_convolution.c in	buffer-overflow exists in the function sbr_qmf.synthesis_64 located in sbr_qmf.c. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32274  An issue was discovered in faad2 through 2.10.0. A NULL pointer dereference exists in the function get_sample() located in output.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-32276  An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function sbr_qmf_analysis_32 located in sbr_qmf_c. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32277  An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function lt_prediction located in lt_predict.c. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32277  An issue was discovered in faad2 through 2.10.0. A heap-buffer-overflow exists in the function lt_prediction located in lt_predict.c. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32278  Integer Overflow vulnerability in function filter16_roberts in libavfilter/vf_convolution.c in git/commit/			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a Denial of Service or other unspecified impacts.  CVE ID: CVE-2021-38090	dd233d4eb2 efa44678a0b c44869f23, https://trac.f fmpeg.org/ti cket/8263	
Integer Overflow or Wraparound	20-Sep-21	6.8	Integer Overflow vulnerability in function filter16_sobel in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.  CVE ID: CVE-2021-38091	https://git.ff mpeg.org/git web/ffmpeg. git/commit/ 99f8d32129 dd233d4eb2 efa44678a0b c44869f23, https://trac.f fmpeg.org/ti cket/8263	A-FFM-FFMP- 061021/114
Integer Overflow or Wraparound	20-Sep-21	6.8	Integer Overflow vulnerability in function filter_prewitt in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.  CVE ID: CVE-2021-38092	https://git.ff mpeg.org/git web/ffmpeg. git/commit/ 99f8d32129 dd233d4eb2 efa44678a0b c44869f23, https://trac.f fmpeg.org/ti cket/8263	A-FFM-FFMP- 061021/115
Integer Overflow or Wraparound	20-Sep-21	6.8	Integer Overflow vulnerability in function filter_robert in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.  CVE ID: CVE-2021-38093	https://git.ff mpeg.org/git web/ffmpeg. git/commit/ 99f8d32129 dd233d4eb2 efa44678a0b c44869f23, https://trac.f fmpeg.org/ti cket/8263	A-FFM-FFMP- 061021/116

Weakness	Publish Date	cvss	Descr	iption & CVE	ID	Pa	itch	NCII	PC ID
Integer Overflow or Wraparound	20-Sep-21	6.8	Integer Over vulnerabilitier_sobelibavfilter/ Ffmpeg 4.2 attackers to Service or impacts.  CVE ID : CV	mpeg. web/f git/co 99f8d dd233 efa446 c4486 https:	//trac.f c.org/ti	A-FFM 06102	-FFMP- 1/117		
ffw									
omgf									
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Sep-21	6.4	before 4.5. or validate parameter which allow unauthents perform parameter with Google Google For	WordPress 4 does not e the handle of the REST ws icated users arbitrary CS e Fonts CSS fonts upload its website.	SAPI,  to l and S file , or ded on	N/A		A-FFW OMGF- 06102	-
Cross-Site Request Forgery (CSRF)	20-Sep-21	5.5	The OMGF WordPress plugin before 4.5.4 does not enforce path validation, authorisation and CSRF checks in the omgf_ajax_empty_dir AJAX action, which allows any authenticated users to delete arbitrary files or folders on the server.  CVE ID: CVE-2021-24639			N/A		A-FFW OMGF- 06102	-
firefly-iii									
firefly_iii									
Cross-Site	27-Sep-21	6.8	firefly-iii is	vulnerable	to	https:	//hunt	A-FIR-	FIRE-
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-	4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	C	escriptio	n & CVE	ID	Pa	tch	NCII	PC ID
Request Forgery (CSRF)			(CSRF)	Site Req			es/data-4ffc-487a4-a2a79e5,https:/b.com/iii/cor/78f3575f31	0bd44 //githu /firefly efly- nmit/5 0498b d321c7 c7f7b3	06102	1/120
flask-restx_pr	oject									
flask-restx										
Uncontrolled Resource Consumption	20-Sep-21	5	flask-r driven RESTP before vulner Expres in ema	sion De	a comm Flask- k-REST 0.5.1 is ReDoS ( nial of S . This is	unity  X  Regular  Service)  fixed in	b.com n- restx/ 372, https: b.com n- restx/ t/bab3 f355d 8fd37 71849 https: b.com	//githu /pytho flask- commi 31e085 d7385 15f7ed 1656da, //githu /advis GHSA-	A-FLA- 06102	
fontsplugin										
fonts									ı	
Improper	20-Sep-21	3.5	The Go	ogle Fo	nts		N/A		A-FON	-FONT-
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')			Typography WordPress plugin before 3.0.3 does not escape and sanitise some of its block settings, allowing users with as role as low as Contributor to perform Stored Cross-Site Scripting attacks via blockType (combined with content), align, color, variant and fontID argument of a Gutenberg block.  CVE ID: CVE-2021-24637		061021/122
frogcms_proje	ect		CVLID: CVL 2021 24037		
frogcms					
Unrestricted Upload of File with Dangerous Type	23-Sep-21	7.5	Privilege escalation in 'upload.php' in FrogCMS SentCMS v0.9.5 allows attacker to execute arbitrary code via crafted php file.  CVE ID: CVE-2021-26794	N/A	A-FRO-FROG- 061021/123
getgrav					
grav					
Reliance on Cookies without Validation and Integrity Checking	27-Sep-21	5	grav is vulnerable to Reliance on Cookies without Validation and Integrity Checking CVE ID: CVE-2021-3818	https://hunt r.dev/bounti es/c2bc65af- 7b93-4020- 886e- 8cdaeb0a58e a	A-GET-GRAV- 061021/124
grav-plugin-a	dmin				
Improper Restriction of Rendered UI Layers or Frames	27-Sep-21	5.8	grav-plugin-admin is vulnerable to Improper Restriction of Rendered UI Layers or Frames CVE ID: CVE-2021-3799	https://hunt r.dev/bounti es/d73f24a8 -302b-4f9f- abb8- 54688abd98 13,	A-GET-GRAV- 061021/125

getshortcodes shortcodes_ult				https://githu b.com/getgra v/grav- plugin- admin/com mit/853abfb bd3c14a0a6 01c941dcfaa 3858b6283b 69	
shortcodes_ult	timate				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The Shortcodes Ultimate WordPress plugin before 5.10.2 allows users with Contributor roles to perform stored XSS via shortcode attributes. Note: the plugin is inconsistent in its handling of shortcode attributes; some do escape, most don't, and there are even some attributes that are insecure by design (like [su_button]'s onclick attribute).  CVE ID: CVE-2021-24525	N/A	A-GET-SHOR- 061021/126
Github					
enterprise_ser	rver				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Sep-21	4	A path traversal vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. Usercontrolled configuration options used by GitHub Pages were not sufficiently restricted and made it possible to read files on the GitHub Enterprise Server	https://docs. github.com/e n/enterprise - server@3.1/ admin/relea se- notes#3.1.8, https://docs. github.com/e n/enterprise	A-GIT-ENTE- 061021/127

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			instance. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.1.8 and was fixed in 3.1.8, 3.0.16, and 2.22.22. This vulnerability was reported via the GitHub Bug Bounty program. This is the result of an incomplete fix for CVE-2021-22867.	- server@3.0/ admin/relea se- notes#3.0.16 , https://docs. github.com/e n/enterprise - server@2.22 /admin/rele ase- notes#2.22.2 2	
Exposure of Resource to Wrong Sphere	24-Sep-21	7.5	An improper access control vulnerability in GitHub Enterprise Server allowed a workflow job to execute in a self-hosted runner group it should not have had access to. This affects customers using self-hosted runner groups for access control. A repository with access to one enterprise runner group could access all of the enterprise runner groups within the organization because of improper authentication checks during the request. This could cause code to be run unintentionally by the incorrect runner group. This vulnerability affected GitHub Enterprise Server versions from 3.0.0 to 3.0.15 and 3.1.0 to 3.1.7 and was fixed in	https://docs.github.com/en/enterprise-server@3.1/admin/release-notes#3.1.8, https://docs.github.com/en/enterprise-server@3.0/admin/release-notes#3.0.16	A-GIT-ENTE- 061021/128

6-7

8-9

7-8

2-3 3-4 4-5

CVSS Scoring Scale

)-Sep-21	4.3	3.0.16 and 3.1.8 releases.  CVE ID: CVE-2021-22869  An issue was discovered in libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function bit_read_BB() located in bits.c. It allows an	https://githu b.com/Libre	
)-Sep-21	4.3	An issue was discovered in libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function bit_read_BB()		
)-Sep-21	4.3	libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function bit_read_BB()		
)-Sep-21	4.3	libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function bit_read_BB()		
)-Sep-21	4.3	libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function bit_read_BB()		
		attacker to cause Denial of Service.  CVE ID: CVE-2021-39521	DWG/libred wg/issues/2 62	A-GNU-LIBR- 061021/129
)-Sep-21	6.8	An issue was discovered in libredwg through v0.10.1.3751. bit_wcs2len() in bits.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39522	https://githu b.com/Libre DWG/libred wg/issues/2 55	A-GNU-LIBR- 061021/130
)-Sep-21	4.3	An issue was discovered in libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function check_POLYLINE_handles() located in decode.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39523	N/A	A-GNU-LIBR- 061021/131
)-Sep-21	6.8	An issue was discovered in libredwg through v0.10.1.3751. bit_read_fixed() in bits.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39525	N/A	A-GNU-LIBR- 061021/132
)-Sep-21	6.8	An issue was discovered in libredwg through	N/A	A-GNU-LIBR- 061021/133
)	-Sep-21	-Sep-21 4.3 -Sep-21 6.8	An issue was discovered in libredwg through v0.10.1.3751. bit_wcs2len() in bits.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39522  An issue was discovered in libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function check_POLYLINE_handles() located in decode.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39523  An issue was discovered in libredwg through v0.10.1.3751. bit_read_fixed() in bits.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39525  -Sep-21  6.8  An issue was discovered in libredwg through v0.10.1.3751. bit_read_fixed() in bits.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39525	An issue was discovered in libredwg through v0.10.1.3751. bit_wcs2len() in bits.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39522  An issue was discovered in libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function check_P0LYLINE_handles() located in decode.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39523  An issue was discovered in libredwg through v0.10.1.3751. bit_read_fixed() in bits.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39525  -Sep-21  6.8  An issue was discovered in libredwg through N/A

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pa	tch	NCI	IPC ID
Write				o_privat teap-bas	te() in de					
			CVE ID	) : CVE-	2021-39	9527				
Double Free	20-Sep-21	6.8	libredy v0.10.1 dwg_fr ) in dw free.	wg throi 1.3751. ree_MAT vg.spec l		private( uble	b.com/	libred		J-LIBR- 21/134
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in libredwg through v0.10.1.3751. bit_wcs2nlen() in bits.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39530				https://b.com/ DWG/I wg/iss 58	libred		J-LIBR- 21/135
ncurses				_						
Out-of- bounds Write	20-Sep-21	6.8	ncurse _nc_cap has a h overflo	An issue was discovered in ncurses through v6.2-1nc_captoinfo in captoinfo.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39537			ive/ht	g/arch ml/bu s/202		J-NCUR- 21/136
goteleport										
teleport										
Improper Authenticati on	18-Sep-21	7.5	Teleport before 4.4.11, 5.x before 5.2.4, 6.x before 6.2.12, and 7.x before 7.1.1 allows forgery of SSH host certificates in some situations.  CVE ID: CVE-2021-41393				b.com/ ational ort/rel tag/v6 https:/ b.com/ ational	/telep leases/ .2.12, //githu /gravit	A-GOT-TELE- 061021/137	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				tag/v4.4.11, https://githu b.com/gravit ational/telep ort/releases/ tag/v5.2.4, https://githu b.com/gravit ational/telep ort/releases/ tag/v7.1.1	
N/A	18-Sep-21	5	Teleport before 4.4.11, 5.x before 5.2.4, 6.x before 6.2.12, and 7.x before 7.1.1 allows alteration of build artifacts in some situations.  CVE ID: CVE-2021-41394	https://github.com/gravitational/teleport/releases/tag/v6.2.12,https://github.com/gravitational/teleport/releases/tag/v4.4.11,https://github.com/gravitational/teleport/releases/tag/v5.2.4,https://github.com/gravitational/teleport/releases/tag/v7.1.1	A-GOT-TELE- 061021/138
N/A	18-Sep-21	6.4	Teleport before 6.2.12 and 7.x before 7.1.1 allows attackers to control a database connection string, in some situations, via a crafted database name or username.  CVE ID: CVE-2021-41395	https://githu b.com/gravit ational/telep ort/releases/ tag/v6.2.12, https://githu b.com/gravit ational/telep ort/releases/	A-GOT-TELE- 061021/139

6-7

8-9

7-8

2-3 3-4 4-5

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				tag/v7.1.1	
gpac					
gpac					
Out-of- bounds Write	20-Sep-21	6.8	Buffer overflow vulnerability in function gf_fprintf in os_file.c in gpac before 1.0.1 allows attackers to execute arbitrary code. The fixed version is 1.0.1.  CVE ID: CVE-2021-32268	https://githu b.com/gpac/ gpac/issues/ 1587	A-GPA-GPAC- 061021/140
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in gpac through 20200801. A NULL pointer dereference exists in the function ilst_item_box_dump located in box_dump.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-32269	N/A	A-GPA-GPAC- 061021/141
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in gpac through 20200801. A NULL pointer dereference exists in the function vwid_box_del located in box_code_base.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-32270	N/A	A-GPA-GPAC- 061021/142
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in gpac through 20200801. A stack-buffer-overflow exists in the function DumpRawUIConfig located in odf_dump.c. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32271	N/A	A-GPA-GPAC- 061021/143

6-7

8-9

7-8

2-3 3-4 4-5

CVSS Scoring Scale

Weakness	Publish Date	cvss	D	escriptio	on & CVE	ID	Pa	tch	NCII	PC ID
Gradle										
gradle										
Exposure of Sensitive Information to an Unauthorize d Actor	24-Sep-21	5	2021.1 unauth respon- disclosi sensitiv details) request Enterpi header	.3 can a orized se (info ure of point o	rise beformation on the configurated Here X-Grante Archer 2021-4	of a uration ITTP adle- est	rity.gr	//secu adle.co visory/ 02	A-GRA 06102	-GRAD- 1/144
Server-Side Request Forgery (SSRF)	24-Sep-21	5	2021.1 ability that attacks the syst	ability to perform SSRF attacks can potentially reset				//secu adle.co visory/ 05	A-GRA 06102	-GRAD- 1/145
Server-Side Request Forgery (SSRF)	24-Sep-21	5	2021.1 ability attacks discove resource	In Gradle Enterprise before 2021.1.3, an attacker with the ability to perform SSRF attacks can potentially				//secu adle.co visory/ 04	A-GRA 06102	-GRAD- 1/146
Deserializati on of Untrusted Data	24-Sep-21	6.8	In Gradle Enterprise before 2021.1.3, a crafted request can trigger deserialization of arbitrary unsafe Java objects. The attacker must have the encryption and signing keys.  CVE ID: CVE-2021-41588				rity.gr	//secu adle.co visory/ 03	A-GRA 06102	-GRAD- 1/147
grame									ı	
faust										
NULL Pointer	20-Sep-21	4.3			liscover v2.30.5.	ed in A NULL	N/A		A-GRA 06102	-FAUS- 1/148
CVSS 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	on & CVE	ID	Pa	tch	NCI	IPC ID		
Dereference			the fun CosPri ) locat allows	er derefenction im::com ed in co an attac of Servi	puteSig sprim.h cker to c	Output( h. It						
			CVE II	D : CVE-	2021-3	2275						
Gurock												
testrail	testrail											
Incorrect Authorizatio n	22-Sep-21	5	Guroc 7.2.0.3 sensit: exposi access the cli TestRa disclos applic corres be test result hardce keys, o	per Acco k TestRa 3014 res ive infor ure. A th the /file ent side ail applie sing a fu ation file sponding ted, and in the di oded cre or other	nil version ulted in mation reat act es.md5 for of a Gurantion, ll list of es and the grile pattin some isclosuredentials sensitiv	or can file on rock  ne ths. The chs can cases, e of s, API ce data.	-	ock.co crail/to cerpris		R-TEST- 1/149		
gutenslider												
gutenslider												
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	Guten 5.2.0 c minW Guten allow as con Cross-	ordPresslider places not idth attraces wisers wieributors Site Script : CVE-	ugin being escape of the city which is a role to perfect of the city at the ci	fore the a ch could e as low orm tacks	N/A			'-GUTE- 1/150		
hcxtools_proj	hcxtools_project											
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID				
hcxtoold									
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in hcxtools through 6.1.6. A global-buffer-overflow exists in the function pcapngoptionwalk located in hcxpcapngtool.c. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32286	https://githu b.com/ZerBe a/hcxtools/is sues/155	A-HCX-HCXT- 061021/151				
IBM									
aspera_on_cloud									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Aspera Cloud is vulnerable to stored crosssite 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: 208343.  CVE ID: CVE-2021-38870	https://ww w.ibm.com/s upport/page s/node/6491 603, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/208343	A-IBM-ASPE- 061021/152				
business_aute	 omation_wor	kflow							
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	29-Sep-21	3.5	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3,20.0.0.1, 20.0.0.2, and 21.0.2 and IBM Business Process Manager 8.5 and 8.6 are vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	https://ww w.ibm.com/s upport/page s/node/6493 271, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204832	A-IBM-BUSI- 061021/153				

1-2

0-1

5-6

6-7

7-8

8-9

9-10

			functionality potentially		
business_proce	ess manage	r	leading to credentials disclosure within a trusted session. IBM X-Force ID: 204832.  CVE ID: CVE-2021-29834		
	eoo_manage	•	IBM Business Automation		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	29-Sep-21	3.5	Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3,20.0.0.1, 20.0.0.2, and 21.0.2 and IBM Business Process Manager 8.5 and 8.6 are vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204832.	https://ww w.ibm.com/s upport/page s/node/6493 271, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204832	A-IBM-BUSI- 061021/154
1 1 1 6	1		CVE ID : CVE-2021-29834		
cloud_pak_for_	_data				
Exposure of Sensitive Information to an Unauthorize d Actor	20-Sep-21	2.1	IBM Cloud Pak for Data 2.5 could allow a local user with special privileges to obtain highly sensitive information. IBM X-Force ID: 209575.  CVE ID: CVE-2021-38899	https://ww w.ibm.com/s upport/page s/node/6490 435	A-IBM-CLOU- 061021/155
db2					
Exposure of Sensitive Information to an Unauthorize	16-Sep-21	3.5	IBM Db2 11.2 and 11.5 contains an information disclosure vulnerability, exposing remote storage credentials to privileged	https://ww w.ibm.com/s upport/page s/node/6489 489,	A-IBM-DB2- 061021/156
CVSS Scoring Scale	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
d Actor			users under specific conditions. IBM X-Fporce ID: 201780. CVE ID: CVE-2021-29752	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/201780	
Allocation of Resources Without Limits or Throttling	16-Sep-21	1.9	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267.  CVE ID: CVE-2021-29763	https://ww w.ibm.com/s upport/page s/node/6489 493, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/202267	A-IBM-DB2- 061021/157
Exposure of Sensitive Information to an Unauthorize d Actor	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470.  CVE ID: CVE-2021-29825	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204470, https://ww w.ibm.com/s upport/page s/node/6489 499	A-IBM-DB2- 061021/158
jazz_for_servi	ce_managem	ent			
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/208405, https://ww w.ibm.com/s upport/page s/node/6491 521	A-IBM-JAZZ- 061021/159

1-2

0-1

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session. IBM X-Force ID: 208405.		
			CVE ID : CVE-2021-38877		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Tivoli Netcool/OMNIbus_GUI and IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.  CVE ID: CVE-2021-29800	https://ww w.ibm.com/s upport/page s/node/6491 109, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/203906	A-IBM-JAZZ- 061021/160
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204279.  CVE ID: CVE-2021-29810	https://ww w.ibm.com/s upport/page s/node/6491 547, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204279	A-IBM-JAZZ- 061021/161
Improper Neutralizatio n of Input During Web Page	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross-	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204330,	A-IBM-JAZZ- 061021/162

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204330.  CVE ID: CVE-2021-29812	https://ww w.ibm.com/s upport/page s/node/6491 545	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204331.  CVE ID: CVE-2021-29813	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204331, https://ww w.ibm.com/s upport/page s/node/6491 543	A-IBM-JAZZ- 061021/163
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted	https://ww w.ibm.com/s upport/page s/node/6491 539, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204334	A-IBM-JAZZ- 061021/164

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			session. IBM X-Force ID: 204334.		
			CVE ID : CVE-2021-29814		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204340.  CVE ID: CVE-2021-29815	https://ww w.ibm.com/s upport/page s/node/6491 537, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204340	A-IBM-JAZZ- 061021/165
Cross-Site Request Forgery (CSRF)	23-Sep-21	4.3	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI 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: 204341.  CVE ID: CVE-2021-29816	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204341, https://ww w.ibm.com/s upport/page s/node/6491 535	A-IBM-JAZZ- 061021/166
Improper Restriction of XML External Entity Reference	21-Sep-21	5.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker	https://ww w.ibm.com/s upport/page s/node/6490 905	A-IBM-JAZZ- 061021/167

1-2

0-1

5-6

6-7

7-8

8-9

9-10

Weakness	<b>Publish Date</b>	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 204775.  CVE ID: CVE-2021-29831		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204824.  CVE ID: CVE-2021-29832	https://ww w.ibm.com/s upport/page s/node/6491 529, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204824	A-IBM-JAZZ- 061021/168
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204825.  CVE ID: CVE-2021-29833	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204825, https://ww w.ibm.com/s upport/page s/node/6491 527	A-IBM-JAZZ- 061021/169
	23-Sep-21	2.1	IBM Jazz for Service	https://ww	A-IBM-JAZZ-

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
Storage of Sensitive Information			IBM T Netco displa plain o read b Force	gement 1 ivoli ol/OMN ys user o clear tex by a local ID: 2076 D: CVE-2	Ibus_GU credenti t which user. IB 510.	I als in can be BM X-	525, https:/ ange.xi	z/page e/6491 //exch force.i ud.com rabiliti	06102	1/170
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	Manag IBM T Netco vulner script allows arbitr the W intend poten creder a trus Force	azz for Segement 1 ivoli ol/OMNI rable to oling. This is users to ary Javas eb UI thu ded funct tially lea ntials dis ted sessi ID: 2076	Ibus_GU cross-site vulnerate cembed Script cous alterinationality ding to sclosure on. IBM	I is te bility de in ng the within X-	523, https://ange.xi	com/s c/page e/6491 //exch force.i ud.com rabiliti		-JAZZ- 1/171
security_guar	dium									
Generation of Error Message Containing Sensitive Information	23-Sep-21	4	could to obt inform technic return inform further system 19556	ecurity ( allow a rain sension wation wation contacts and in the nation contacts ar attacks b. IBM X 59.  CVE-2	remote a itive hen a de r messag e brows ould be u s against -Force Il	etailed ge is er. This ised in the D:	125, https:/ ange.xi	com/s c/page e/6491 //exch force.i ud.com rabiliti		-SECU- 1/172
security_verif	fy_bridge									
Insufficiently Protected	23-Sep-21	2.1		ecurity V ) stores i			https:/ ange.x	-	A-IBM	-SECU-
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Credentials			in plain clear text which can be read by a locally authenticated user. IBM X- Force ID: 208154. CVE ID: CVE-2021-38863	bmcloud.com /vulnerabiliti es/208154, https://ww w.ibm.com/s upport/page s/node/6491 653	061021/173
Improper Certificate Validation	23-Sep-21	5	IBM Security Verify Bridge 1.0.5.0 could allow a user to obtain sensitive information due to improper certificate validation. IBM X-Force ID: 208155.  CVE ID: CVE-2021-38864	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/208155, https://ww w.ibm.com/s upport/page s/node/6491 651	A-IBM-SECU- 061021/174
Insufficiently Protected Credentials	23-Sep-21	2.1	IBM Security Verify Bridge 1.0.5.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 196346.  CVE ID: CVE-2021-20434	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/196346, https://ww w.ibm.com/s upport/page s/node/6491 651	A-IBM-SECU- 061021/175
Improper Certificate Validation	23-Sep-21	2.1	IBM Security Verify Bridge 1.0.5.0 does not properly validate a certificate which could allow a local attacker to obtain sensitive information that could aid in further attacks against the system. IBM X-Force ID: 196355.  CVE ID: CVE-2021-20435	https://ww w.ibm.com/s upport/page s/node/6491 651, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/196355	A-IBM-SECU- 061021/176
sterling_file_g	gateway			•	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Sterling File Gateway 2.2.0.0 through 6.1.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 197666.	https://ww w.ibm.com/s upport/page s/node/6491 647, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/197666	A-IBM-STER- 061021/177
Generation of Error Message Containing Sensitive Information	23-Sep-21	4	IBM Sterling File Gateway 2.2.0.0 through 6.1.0.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 197667.  CVE ID: CVE-2021-20485	https://ww w.ibm.com/s upport/page s/node/6491 645, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/197667	A-IBM-STER- 061021/178
Exposure of Sensitive Information to an Unauthorize d Actor	23-Sep-21	4	IBM Sterling File Gateway 2.2.0.0 through 6.1.0.3 could allow a remote authenciated user to obtain sensitive information. By sending a specially crafted request, the user could disclose a valid filepath on the server which could be used in further attacks against the system. IBM X-Force ID: 199234.  CVE ID: CVE-2021-20563	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/199234, https://ww w.ibm.com/s upport/page s/node/6491 645	A-IBM-STER- 061021/179
sterling_orde	r_manageme	nt			
	30-Sep-21	4.3	IBM Sterling Order	https://ww	A-IBM-STER-

Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')  tivoli_netcool\\/on  Improper Restriction of XML External Entity Reference  tivoli_netcool\\/on  Improper Neutralizatio n of Input			Management 9.4, 9.5, and 10.0 is vulnerable to cross- site scripting. This vulnerability allows users to	w.ibm.com/s upport/page	061021/180
Improper Restriction of XML External Entity Reference  tivoli_netcool\\/on  Improper Neutralizatio			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: 199179.  CVE ID: CVE-2021-20554	s/node/6493 881	
Restriction of XML External Entity Reference  tivoli_netcool\\/on Improper Neutralizatio	nnibus_	gui			
Improper Neutralizatio	ep-21	5.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 204775.  CVE ID: CVE-2021-29831	https://ww w.ibm.com/s upport/page s/node/6490 905	A-IBM-TIVO- 061021/181
Neutralizatio	nnibus_	webgu	i		
During Web Page Generation ('Cross-site Scripting')	ep-21	3.5	IBM Tivoli Netcool/OMNIbus_GUI and IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	https://ww w.ibm.com/s upport/page s/node/6491 109, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/203906	A-IBM-TIVO- 061021/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functionality potentially leading to credentials disclosure within a trusted session.  CVE ID: CVE-2021-29800		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored crosssite 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: 204264.  CVE ID: CVE-2021-29806	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204264, https://ww w.ibm.com/s upport/page s/node/6490 747	A-IBM-TIVO- 061021/183
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored crosssite 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: 204265.  CVE ID: CVE-2021-29807	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204265, https://ww w.ibm.com/s upport/page s/node/6490 747	A-IBM-TIVO- 061021/184
Improper Neutralizatio n of Input During Web	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross-	https://exch ange.xforce.i bmcloud.com /vulnerabiliti	A-IBM-TIVO- 061021/185

1-2

0-1

5-6

6-7

8-9

9-10

7-8

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204269.  CVE ID: CVE-2021-29808	es/204269, https://ww w.ibm.com/s upport/page s/node/6490 747	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204270.  CVE ID: CVE-2021-29809	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204270, https://ww w.ibm.com/s upport/page s/node/6490 747	A-IBM-TIVO- 061021/186
Insufficiently Protected Credentials	20-Sep-21	4	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 stores user credentials in plain clear text which can be read by an authenticated admin user. IBM X-Force ID: 204329.  CVE ID: CVE-2021-29811	https://ww w.ibm.com/s upport/page s/node/6490 747, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204329	A-IBM-TIVO- 061021/187
Improper Neutralizatio n of Input	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0	https://exch ange.xforce.i bmcloud.com	A-IBM-TIVO- 061021/188

6-7

7-8

8-9

2-3 3-4 4-5

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204343.  CVE ID: CVE-2021-29817	/vulnerabiliti es/204343, https://ww w.ibm.com/s upport/page s/node/6490 747	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 204345.  CVE ID: CVE-2021-29818	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204345, https://ww w.ibm.com/s upport/page s/node/6490 747	A-IBM-TIVO- 061021/189
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 204346.  CVE ID: CVE-2021-29819	https://ww w.ibm.com/s upport/page s/node/6490 747	A-IBM-TIVO- 061021/190

6-7

7-8

8-9

2-3 3-4 4-5

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 204347.  CVE ID: CVE-2021-29820	https://ww w.ibm.com/s upport/page s/node/6490 747	A-IBM-TIVO- 061021/191
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	IBM Jazz for Service Management and IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 204348.  CVE ID: CVE-2021-29821	https://ww w.ibm.com/s upport/page s/node/6490 747, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204348	A-IBM-TIVO- 061021/192
N/A	20-Sep-21	4	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 could allow an authenticated usre to cause a denial of service through the WebGUI Map Creation page. IBM X- Force ID: 205685.  CVE ID: CVE-2021-29856	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/205685, https://ww w.ibm.com/s upport/page s/node/6490 747	A-IBM-TIVO- 061021/193
websphere_a	pplication_se	rver			

1-2

0-1

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authenticati on Attempts	16-Sep-21	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0 and Liberty 17.0.0.3 through 21.0.0.9 could allow a remote user to enumerate usernames due to a difference of responses from valid and invalid login attempts. IBM X- Force ID: 205202.  CVE ID: CVE-2021-29842	https://ww w.ibm.com/s upport/page s/node/6489 485, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/205202	A-IBM-WEBS- 061021/194
inflect_projec	t				
inflect					
Incorrect Comparison	27-Sep-21	5	inflect is vulnerable to Inefficient Regular Expression Complexity CVE ID: CVE-2021-3820	https://githu b.com/pksun kara/inflect/ commit/a9a 0a8e9561c3 487854c7cae 42565d9652 ec858b, https://hunt r.dev/bounti es/4612b31a -072b-4f61- a916- c7e4cbc2042 a	A-INF-INFL- 061021/195
itservicejung					
youforms-fre	e-for-copeca	rt			
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The youForms for WordPress plugin through 1.0.5 does not sanitise escape the Button Text field of its Templates, allowing high privilege users (editors and admins) to perform Cross-Site Scripting attacks even when the unfiltered_html capability is	N/A	A-ITS-YOUF- 061021/196

Weakness	Publish Date	cvss	1	Description	n & CVE	ID	Pa	tch	NCI	IPC ID
			disallo	wed						
			CVE II	D : CVE-	2021-24	<b>4596</b>				
jpeg										
libjpeg										
Incorrect Comparison	20-Sep-21	4.3	libjpeg uncau except ACLos locate It allo	ue was c g throug ght float tion in the sslessSca d in aclo ws an at	h 20200 ing poir ne functi n::Parse sslesssc tacker to	21. An at on eMCU() an.cpp.	N/A	N/A		-LIBJ- 21/197
			CVE II	D : CVE-	2021-39	9514				
NULL Pointer Dereference	20-Sep-21	4.3	libjpeg NULL exists Sampl rseMC sampl It allow Denial	ue was on the furth of the furth of Servine was an attention of Servine was attention of	h 20200 dereferenction avedLSS ted in avedlsso tacker to	21. A ence Scan::Pa an.cpp.	N/A		A-JPE- 06102	-LIBJ- 21/198
			CVE II	D : CVE-	2021-39	9515				
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function HuffmanDecoder::Get() located in huffmandecoder.hpp. It allows an attacker to cause Denial of Service.		N/A		A-JPE- 06102	-LIBJ- 21/199		
			CVE II	D : CVE-	2021-39	9516				
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::Reco		b.com,	//githu /thorfd ipeg/is	A-JPE- 06102	-LIBJ- 21/200		
CVSS Scoring Sca	ile <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			nstructUnsampled() located in blockbitmaprequester.cpp. It allows an attacker to cause Denial of Service.		
			CVE ID : CVE-2021-39517		
Out-of- bounds Write	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. LineBuffer::FetchRegion() in linebuffer.cpp has a heapbased buffer overflow.  CVE ID: CVE-2021-39518	https://githu b.com/thorfd bg/libjpeg/is sues/35	A-JPE-LIBJ- 061021/201
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::PullQ Data() located in blockbitmaprequester.cpp It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39519	https://githu b.com/thorfd bg/libjpeg/is sues/28	A-JPE-LIBJ- 061021/202
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::Push ReconstructedData() located in blockbitmaprequester.cpp. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39520	https://githu b.com/thorfd bg/libjpeg/is sues/34	A-JPE-LIBJ- 061021/203
jscom					
revoworks_bi	rowser				
Exposure of Resource to Wrong Sphere	17-Sep-21	6.8	Improper control of program execution vulnerability in RevoWorks Browser 2.1.230 and earlier allows an attacker to execute an arbitrary	https://jsco m.jp/news- 20210910_2 /	A-JSC-REVO- 061021/204
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE II	D	Pat	tch	NCII	PC ID
			command or code via unspecified vectors.  CVE ID: CVE-2021-207	790				
Improper Privilege Management	17-Sep-21	6.4	Improper access control vulnerability in RevoWo Browser 2.1.230 and ear allows an attacker to by access restriction and to exchange unauthorized between the local environment and the ison environment or settings the web browser via unspecified vectors.  CVE ID: CVE-2021-207	orks arlier ypass o files olated s of	https://jsco m.jp/news- 20210910_2 /		A-JSC-: 06102	
jsoneditoronline								
jsoneditor								
Incorrect Comparison	27-Sep-21	5	jsoneditor is vulnerable Inefficient Regular Expression Complexity <b>CVE ID : CVE-2021-38</b> 2		https://b.com/ong/jsor/com/92e3862a145617da86ed0676https:/r.dev/les/1e3/b7ed-a4ea-c4c7563	josdej onedit nmit/0 6cf49f 06256 e0137 c3e, j/hunt oounti ed803 42f1-	A-JSO- 06102	
jsoniter jsoniter								
Deserializati on of Untrusted Data	19-Sep-21	7.5	All versions of package com.jsoniter:jsoniter ar vulnerable to Deserializ of Untrusted Data via	zation	N/A	7.0	A-JSO- 06102	1/207
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			malicious JSON strings. This may lead to a Denial of Service, and in certain cases, code execution.		
			CVE ID : CVE-2021-23441		
jsuites					
jsuites					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-21	3.5	jsuites is an open source collection of common required javascript web components. In affected versions users are subject to cross site scripting (XSS) attacks via clipboard content. jsuites is vulnerable to DOM based XSS if the user can be tricked into copying _anything_ from a malicious and pasting it into the html editor. This is because a part of the clipboard content is directly written to `innerHTML` allowing for javascript injection and thus XSS. Users are advised to update to version 4.9.11 to resolve.  CVE ID: CVE-2021-41086	https://github.com/jsuites/commit/fe1d3cc5e339f2f4da8ed1f9f42271fdf9cbd8d2,https://github.com/jsuites/jsuites/security/advisories/GHSA-qh7x-j4v8-qw5w,https://github.com/jsuites/jsuites/commit/d47a6f4e143188dde2742f4cffd313e1068ad3b3	A-JSU-JSUI- 061021/208
Juniper					
libslax			An icoup was discovered in		
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in libslax through v0.22.1. slaxLexer() in slaxlexer.c has a stack-based buffer overflow.  CVE ID: CVE-2021-39531	N/A	A-JUN-LIBS- 061021/209

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libslax through v0.22.1. A NULL pointer dereference exists in the function slaxLexer() located in slaxlexer.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39532	N/A	A-JUN-LIBS- 061021/210
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in libslax through v0.22.1. slaxLexer() in slaxlexer.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39533	N/A	A-JUN-LIBS- 061021/211
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in libslax through v0.22.1. slaxIsCommentStart() in slaxlexer.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39534		A-JUN-LIBS- 061021/212
kindsoft					
kindeditor					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-21	4.3	Cross Site Scripting (XSS) vulnerability exists in all versions of KindEditor, which can be exploited by an attacker to obtain user cookie information.  CVE ID : CVE-2021-37267		A-KIN-KIND- 061021/213
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-21	4.3	Cross Site Scripting (XSS) vulnerability exists in KindEditor (Chinese versions) 4.1.12, which can be exploited by an attacker to obtain user cookie information.  CVE ID: CVE-2021-30086	N/A	A-KIN-KIND- 061021/214
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Kubernetes					
kubernetes					
Externally Controlled Reference to a Resource in Another Sphere	20-Sep-21	3.5	A security issue was discovered with Kubernetes that could enable users to send network traffic to locations they would otherwise not have access to via a confused deputy attack.  CVE ID: CVE-2021-25740	https://githu b.com/kuber netes/kuber netes/issues /103675	A-KUB-KUBE- 061021/215
Files or Directories Accessible to External Parties	20-Sep-21	5.5	A security issue was discovered in Kubernetes where a user may be able to create a container with subpath volume mounts to access files & directories outside of the volume, including on the host filesystem.  CVE ID: CVE-2021-25741	https://githu b.com/kuber netes/kuber netes/issues /104980	A-KUB-KUBE- 061021/216
libiff_project					
libiff					
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in libiff through 20190123. A global-buffer-overflow exists in the function IFF_errorId located in error.c. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32298	N/A	A-LIB-LIBI- 061021/217
libxsmm_proj	ect				
libxsmm					
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in libxsmm through v1.16.1-93. A NULL pointer dereference exists in JIT code. It allows an attacker to cause Denial of	N/A	A-LIB-LIBX- 061021/218
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service.		
			CVE ID : CVE-2021-39535		
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in libxsmm through v1.16.1-93. The JIT code has a heapbased buffer overflow.  CVE ID: CVE-2021-39536	N/A	A-LIB-LIBX- 061021/219
lief-project					
lief					
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in LIEF through 0.11.4. A heap-buffer-overflow exists in the function main located in pe_reader.c. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32297	https://githu b.com/lief- project/LIEF /issues/449	A-LIE-LIEF- 061021/220
limit_login_at	  tempts_proje	ect			
limit_login_at	tempts				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	4.3	The Limit Login Attempts WordPress plugin before 4.0.50 does not escape the IP addresses (which can be controlled by attacker via headers such as X- Forwarded-For) of attempted logins before outputting them in the reports table, leading to an Unauthenticated Stored Cross-Site Scripting issue.  CVE ID: CVE-2021-24657	N/A	A-LIM-LIMI- 061021/221
Linuxfoundat	ion				
tremor					
Use After Free	17-Sep-21	7.5	Tremor is an event processing system for unstructured data. A	https://githu b.com/tremo r-rs/tremor-	A-LIN-TREM- 061021/222
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10
			Page 81 of 861		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSS	vulnerability exists between versions 0.7.2 and 0.11.6. This vulnerability is a memory safety Issue when using `patch` or `merge` on `state` and assign the result back to `state`. In this case, affected versions of Tremor and the tremor-script crate maintains references to memory that might have been freed already. And these memory regions can be accessed by retrieving the `state`, e.g. send it over TCP or HTTP. This requires the Tremor server (or any other program using tremor-script) to execute a tremor-script script that uses the mentioned language construct. The issue has been patched in version 0.11.6 by removing the optimization and always cloning the target expression of a Merge or Patch. If an upgrade is not possible, a possible workaround is to avoid the optimization by introducing a temporary variable and not immediately reassigning to	runtime/pull /1217, https://githu b.com/tremo r-rs/tremor- runtime/com mit/1a2efcd be68e5e7fd0 a05836ac32 d2cde78a0b 2e, https://githu b.com/tremo r-rs/tremor- runtime/sec urity/adviso ries/GHSA- mc22-5q92- 8v85	NCIIPC ID
			`state`.  CVE ID : CVE-2021-39228		
linuxsampler			G. E. I.D. 1. G. V.E. 2021-37220		
libgig					
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in libgig through 20200507. A heap-buffer-overflow exists in the function	N/A	A-LIN-LIBG- 061021/223
CVSS Scoring Scal	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
lodash			RIFF::List::GetSubList located in RIFF.cpp. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32294			
lodash						
Improper Neutralizatio n of Special Elements used in a Command ('Command Injection')	30-Sep-21	7.5	** DISPUTED ** A command injection vulnerability in Lodash 4.17.21 allows attackers to achieve arbitrary code execution via the template function. This is a different parameter, method, and version than CVE-2021-23337. NOTE: the vendor's position is that it's the developer's responsibility to ensure that a template does not evaluate code that originates from untrusted input.  CVE ID: CVE-2021-41720	N/A	A-LOD-LODA- 061021/224	
maianaffiliate						
				I	I	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-21	3.5	MaianAffiliate v1.0 allows an authenticated administrative user to save an XSS to the database.  CVE ID: CVE-2021-39404	N/A	A-MAI-MAIA- 061021/225	
Maianscriptworld						
maianaffiliate	9					
Improper Neutralizatio	20-Sep-21	3.5	MaianAffiliate v.1.0 is suffers from code injection by adding	https://ww w.maianscrip	A-MAI-MAIA- 061021/226	
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 83 of 861	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			a new product via the admin panel. The injected payload is reflected on the affiliate main page for all authenticated and unauthenticated visitors.  CVE ID: CVE-2021-39402	tworld.co.uk /	
Manageengin desktop_cent					
Improper Neutralizatio n of Special Elements used in a Command ('Command Injection')	21-Sep-21	7.5	ManageEngine Desktop Central before build 10.0.683 allows Unauthenticated Remote Code Execution during communication with Notification Server.  CVE ID: CVE-2021-28960	https://ww w.manageen gine.com/pr oducts/deskt op- central/unau thenticated- command- injection- vulnerability.	A-MAN-DESK- 061021/227
Mcafee					
data_loss_pre	vention_disc	over			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Sep-21	6	A buffer overflow vulnerability in McAfee Data Loss Prevention (DLP) Discover prior to 11.6.100 allows an attacker in the same network as the DLP Discover to execute arbitrary code through placing carefully constructed Ami Pro (.sam) files onto a machine and having DLP Discover scan it, leading to remote code execution with elevated privileges. This is caused by the destination buffer being of fixed size and incorrect checks being made on the	https://kc.m cafee.com/co rporate/inde x?page=cont ent&id=SB10 368	A-MCA- DATA- 061021/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			source size.						
			CVE ID : CVE-2021-31845						
data_loss_prevention_endpoint									
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Sep-21	4.6	A buffer overflow vulnerability in McAfee Data Loss Prevention (DLP) Endpoint for Windows prior to 11.6.200 allows a local attacker to execute arbitrary code with elevated privileges through placing carefully constructed Ami Pro (.sam) files onto the local system and triggering a DLP Endpoint scan through accessing a file. This is caused by the destination buffer being of fixed size and incorrect checks being made on the source size.	https://kc.m cafee.com/co rporate/inde x?page=cont ent&id=SB10 368	A-MCA- DATA- 061021/229				
endpoint_secu	ırity		CVE ID : CVE-2021-31844						
Improper Restriction of XML External Entity Reference	17-Sep-21	2.1	XML Entity Expansion injection vulnerability in McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 September 2021 Update allows a local user to initiate high CPU and memory consumption resulting in a Denial of Service attack through carefully editing the EPDeploy.xml file and then executing the setup process.  CVE ID: CVE-2021-31842	https://kc.m cafee.com/co rporate/inde x?page=cont ent&id=SB10 367	A-MCA-ENDP- 061021/230				
Improper Privilege Management	17-Sep-21	4.6	Improper privileges management vulnerability in McAfee Endpoint Security	https://kc.m cafee.com/co rporate/inde	A-MCA-ENDP- 061021/231				
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			(ENS) Windows prior to 10.7.0 September 2021 Update allows local users to access files which they would otherwise not have access to via manipulating junction links to redirect McAfee folder operations to an unintended location.  CVE ID: CVE-2021-31843	x?page=cont ent&id=SB10 367		
mcafee_agent						
Improper Privilege management vulnerability in maconfig for McAfee Agent for Windows prior to 5.7.4 allows a local user to gain access to sensitive information. The utility was able to be run from any location on the file system and by a low privileged user.  CVE ID: CVE-2021-31836  Improper privilege management vulnerability in maconfig for McAfee Agent https://kc.m cafee.com/co rporate/inde x?page=cont ent&id=SB10 369  A-MCA-MCAF-061021/232						
Untrusted Search Path	22-Sep-21	6.9	A DLL sideloading vulnerability in McAfee Agent for Windows prior to 5.7.4 could allow a local user to perform a DLL sideloading attack with an unsigned DLL with a specific name and in a specific location. This would result in the user gaining elevated permissions and the ability to execute arbitrary code as the system user, through not checking the DLL signature.  CVE ID: CVE-2021-31841	https://kc.m cafee.com/co rporate/inde x?page=cont ent&id=SB10 369	A-MCA- MCAF- 061021/233	
Improper Verification	22-Sep-21	6.9	Improper access control vulnerability in the repair	https://kc.m cafee.com/co	A-MCA- MCAF-	

Weakness	Publish Date	CVSS	[	Description	on & CVE	ID	Pa	itch	NCI	PC ID
of Cryptographi c Signature			Windo allow a perfor attack This w of priv execut system correct tempo the rep checki	ss for Mo ows prio a local a m a DLL using un vould res vileges a te arbitr n user, th ctly prote orary dir pair pro- ing the C	r to 5.7.4 ttacker to preload nsigned sult in el nd the a ary code hrough n ecting a ectory u cess and OLL signa	4 could to ding DLLs. levation bility to e as the not lised in a fure.	x?page	te/inde e=cont d=SB10	06102	1/234
Microfocus			CVLII	J.CVE	2021 3.	1017				
arcsight_ente	rprise_secur	ity_ma	nager							
Improper Neutralizatio n of Special Elements used in a Command ('Command Injection')	28-Sep-21	7.5	vulner ArcSig Manag affecti throug could in rem	te Code In the Code In the Enter (ESM) and versing the Exploited to the Code In the Code I	n Micro rprise Se f) produ ons 7.0.: he vulne oited res e execut	Focus ecurity ct, 2 erability ulting ion.	al.mic	//port rofocus s/articl 000001		-ARCS- 1/235
Misp										
misp										
N/A	17-Sep-21	7.5	app/L port.p param a shell	SP before ib/Expo hp mish leter dat l_exec ca D: CVE-	rt/Oper andles a that is lll.	used in	b.com MISP/ t/e36f e741b 0f0c42	//githu /MISP/ commi 73947 cc9732 2199ac cc7051		-MISP- 1/236
mitmproxy										
mitmproxy										
Inconsistent	16-Sep-21	7.5	mitmp	proxy is	an intera	active,	https:/	//githu	A-MIT	-MITM-
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	<b>Description</b>	& CVE ID	Patch	NCI	IPC ID
Interpretatio n of HTTP Requests ('HTTP Request Smuggling')			SSL/TLS-capable proxy. In mitmproxy and below, a male or server is able of HTTP request smattacks through it attacks through it client/server courequest/response mitmproxy as parequest/response message body. We smuggled request captured as part request's body, it appear in the reconstruction of the construction of the construction of the construction. Unlike the control checks of sanitization. Unlike mitmproxy to promitmproxy to promitmproxy to promit management of the construction. Unlike the control checks of sanitization. Unlike the construction of the construction. Unlike the construction of the construction of the construction. Unlike the construction of the construction of the construction. Unlike the construction of the construct	roxy 7.0.2 licious client to perform nuggling mitmproxy. a malicious ald smuggle a se through art of another se's HTTP While a st is still of another t does not quest list and ugh the usual t hooks, w have stom access r input ess one uses rotect an no action is alnerability mitmproxy	b.com/mitm proxy/mitm proxy/securi ty/advisories /GHSA-22gh- 3r9q-xf38	06102	21/237
motopress							
timetable_and	d_event_sche	dule					
Improper Access Control	20-Sep-21	4.3	The Timetable and Event Schedule WordPress plugin before 2.4.2 does not have proper access control when deleting a timeslot, allowing any user with the edit_posts capability (contributor+) to delete arbitrary timeslot from any events. Furthermore, no CSRF check is in place as well,		N/A		T-TIME- 21/238
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5 5-6	6-7 7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			allowing such attack to be performed via CSRF against a logged in with such capability CVE ID: CVE-2021-24583		
Improper Access Control	20-Sep-21	3.5	The Timetable and Event Schedule WordPress plugin before 2.4.2 does not have proper access control when updating a timeslot, allowing any user with the edit_posts capability (contributor+) to update arbitrary timeslot from any events. Furthermore, no CSRF check is in place as well, allowing such attack to be perform via CSRF against a logged in with such capability. In versions before 2.3.19, the lack of sanitisation and escaping in some of the fields, like the descritption could also lead to Stored XSS issues  CVE ID: CVE-2021-24584	N/A	A-MOT-TIME- 061021/239
Exposure of Sensitive Information to an Unauthorize d Actor	20-Sep-21	4	The Timetable and Event Schedule WordPress plugin before 2.4.0 outputs the Hashed Password, Username and Email Address (along other less sensitive data) of the user related to the Even Head of the Timeslot in the response when requesting the event Timeslot data with a user with the edit_posts capability. Combined with the other Unauthorised Event Timeslot Modification issue (https://wpscan.com/reports /submissions/4699/) where	N/A	A-MOT-TIME- 061021/240
CVSS Scoring Sca	ile 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID				
			an arbitrary user ID can be set, this could allow low privilege users with the edit_posts capability (such as author) to retrieve sensitive User data by iterating over the user_id  CVE ID: CVE-2021-24585						
Nagios									
nagios_xi									
Incorrect Default Permissions	28-Sep-21	7.5	Nagios XI before 5.8.5 has Incorrect Permission Assignment for migrate.php.  CVE ID: CVE-2021-36363	https://ww w.nagios.co m/download s/nagios- xi/change- log/, https://asset s.nagios.com /downloads/ nagiosxi/CH ANGES- 5.TXT	A-NAG-NAGI- 061021/241				
Incorrect Default Permissions	28-Sep-21	7.5	Nagios XI before 5.8.5 has Incorrect Permission Assignment for repairmysql.sh.  CVE ID: CVE-2021-36365	https://ww w.nagios.co m/download s/nagios- xi/change- log/, https://asset s.nagios.com /downloads/ nagiosxi/CH ANGES- 5.TXT	A-NAG-NAGI- 061021/242				
netmotionsoft	ware								
mobility									
Incorrect Permission	16-Sep-21	4	The access controls on the Mobility read-only API	https://ww w.netmotion	A-NET-MOBI- 061021/243				
CVSS Scoring Scal	e <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 90 of 861	6-7 7-8	8-9 9-10				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Assignment for Critical Resource			improperly validate user access permissions. Attackers with both network access to the API and valid credentials can read data from it; regardless of access control group membership settings. This vulnerability is fixed in Mobility v11.76 and Mobility v12.14.  CVE ID: CVE-2021-40066	software.co m/security- advisories/c ve-2021- 40066	
Incorrect Permission Assignment for Critical Resource	16-Sep-21	4.9	The access controls on the Mobility read-write API improperly validate user access permissions; this API is disabled by default. If the API is manually enabled, attackers with both network access to the API and valid credentials can read and write data to it; regardless of access control group membership settings. This vulnerability is fixed in Mobility v12.14.  CVE ID: CVE-2021-40067	https://ww w.netmotion software.co m/security- advisories/c ve-2021- 40067	A-NET-MOBI- 061021/244
NI			0.2.2.0.2.2021.0007		
ni-pal					
Improper Input Validation	17-Sep-21	4.6	Improper input validation in the National Instruments NI-PAL driver in versions 20.0.0 and prior may allow a privileged user to potentially enable escalation of privilege via local access.  CVE ID: CVE-2021-38304	https://ww w.ni.com/en- us/support/ documentati on/suppleme ntal/21/imp roper-input- validation- in-ni- pal.html	A-NI-NI-P- 061021/245

Authorizatio n  CVE ID: CVE-2021-34647  Authorizatio n  Author	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
Incorrect Authorizatio n  1	Ninjaforms									
Incorrect Authorizatio n  Incorrect Authorization Incorrect Au	ninja_forms									
Incorrect Authorizatio n  22-Sep-21  4  plugin is vulnerable to arbitrary email sending via the trigger_email_action function found in the ~/includes/Routes/Submissi ons.php file, in versions up to and including 3.5.7. This allows authenticated attackers to send arbitrary emails from the affected server via the /ninja-forms-submissions/email-action REST API which can be used to socially engineer victims.  CVE ID: CVE-2021-34648  plugin is vulnerable to arbitrary email sending via the trigger_email_action https://plugi ns.trac.word press.org/br owser/ninja-forms/trunk /includes/Ro utes/Submis sions.php?re v=2543837# L155	Authorizatio	22-Sep-21	4	plugin is vulnerable to sensitive information disclosure via the bulk_export_submissions function found in the ~/includes/Routes/Submissi ons.php file, in versions up to and including 3.5.7. This allows authenticated attackers to export all Ninja Forms submissions data via the /ninja-forms-submissions/export REST API which can include personally identifiable information.	ns.trac.word press.org/br owser/ninja- forms/trunk /includes/Ro utes/Submis sions.php?re v=2543837#	A-NIN-NINJ- 061021/246				
	Authorizatio	22-Sep-21	4	plugin is vulnerable to arbitrary email sending via the trigger_email_action function found in the ~/includes/Routes/Submissi ons.php file, in versions up to and including 3.5.7. This allows authenticated attackers to send arbitrary emails from the affected server via the /ninja-forms-submissions/email-action REST API which can be used to socially engineer victims.	ns.trac.word press.org/br owser/ninja- forms/trunk /includes/Ro utes/Submis sions.php?re v=2543837#	A-NIN-NINJ- 061021/247				
	nltk			CVE ID: CVE-2021-34048						
nltk										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Comparison	27-Sep-21	5	nltk is vulnerable to Inefficient Regular Expression Complexity CVE ID: CVE-2021-3828	https://hunt r.dev/bounti es/d19aed43 -75bc-4a03- 91a0- 4d0bb516bc 32, https://githu b.com/nltk/ nltk/commit /277711ab1 dec729e626 b27aab6fa35 ea5efbd7e6	A-NLT-NLTK- 061021/248
Nokia					
heif					
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in heif through v3.6.2. A global-buffer-overflow exists in the function HevcDecoderConfigurationRe cord::getPicWidth() located in hevcdecoderconfigrecord.cpp . It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32287	N/A	A-NOK-HEIF- 061021/249
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in heif through v3.6.2. A global-buffer-overflow exists in the function HevcDecoderConfigurationRe cord::getPicHeight() located in hevcdecoderconfigrecord.cpp . It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32288	https://githu b.com/nokiat ech/heif/iss ues/87	A-NOK-HEIF- 061021/250

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
octopus halibut				path/commit /e6bb638ffd d431176701 b3e9024f80 050d0ef0a6	
				https://advis	
Deserializati on of Untrusted Data	22-Sep-21	10	In Halibut versions prior to 4.4.7 there is a deserialisation vulnerability that could allow remote code execution on systems that already trust each other based on certificate verification.  CVE ID: CVE-2021-31819	ories.octopus .com/adv/20 21-08 Remote- Code- Execution- via- Deserialisati on-in-the- Halibut- Protocol- (CVE-2021- 31819).2250 309681.html	A-OCT-HALI- 061021/254
offshorewebn					
availability_ca	alendar				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The Availability Calendar WordPress plugin before 1.2.2 does not sanitise or escape its Category Names before outputting them in page/post where the associated shortcode is embed, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed CVE ID: CVE-2021-24604	N/A	A-OFF-AVAI- 061021/255
Improper	20-Sep-21	6.5	The Availability Calendar	N/A	A-OFF-AVAI-
Improper  CVSS Scoring Sca	Î	6.5 1-2	The Availability Calendar  2-3 3-4 4-5 5-6	6-7 7-8	A-OFF-AVAI- 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')			WordPress plugin before 1.2.1 does not escape the category attribute from its shortcode before using it in a SQL statement, leading to a SQL Injection issue, which can be exploited by any user able to add shortcode to posts/pages, such as contributor+ CVE ID: CVE-2021-24606		061021/256
ombu					
the_sorter					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The check_order function of The Sorter WordPress plugin through 1.0 uses an `area_id` parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.  CVE ID: CVE-2021-24399	N/A	A-OMB-THE 061021/257
Openbsd					
libressl					
Out-of- bounds Read	24-Sep-21	4.3	x509_constraints_parse_mail box in lib/libcrypto/x509/x509_con straints.c in LibreSSL through 3.4.0 has a stack-based buffer over-read. When the input exceeds DOMAIN_PART_MAX_LEN, the buffer lacks '\0' termination.  CVE ID: CVE-2021-41581	https://githu b.com/libres sl- portable/ope nbsd/issues/ 126	A-OPE-LIBR- 061021/258
openssh					
Improper	26-Sep-21	6	sshd in OpenSSH 6.2 through	https://ww	A-OPE-OPEN-
	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
Privilege Management			8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.	w.openssh.co m/txt/releas e-8.8, https://ww w.openssh.co m/security.h tml, https://bugz illa.suse.com /show_bug.c gi?id=11909 75	061021/259			
			CVE ID : CVE-2021-41617					
Openvpn								
openvpn_acce	ess_server			1				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	4.3	OpenVPN Access Server 2.9.0 through 2.9.4 allow remote attackers to inject arbitrary web script or HTML via the web login page URL.  CVE ID: CVE-2021-3824	https://open vpn.net/vpn- server- resources/re lease- notes/#open vpn-access- server-2-9-5	A-OPE-OPEN- 061021/260			
openvpn-mon	nitor_project							
openvpn-mon	nitor							
Cross-Site Request Forgery (CSRF)	27-Sep-21	4.3	furlongm openvpn-monitor through 1.1.3 allows CSRF to disconnect an arbitrary client.  CVE ID: CVE-2021-31604	N/A	A-OPE-OPEN- 061021/261			
Improper Neutralizatio n of Special Elements used in a	27-Sep-21	7.8	furlongm openvpn-monitor through 1.1.3 allows %0a command injection via the OpenVPN management interface socket. This can	N/A	A-OPE-OPEN- 061021/262			
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as a user with access to "Take Attendance" functionality to trigger this vulnerability.  CVE ID: CVE-2021-40309		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	24-Sep-21	3.5	OpenSIS Community Edition version 8.0 is affected by a cross-site scripting (XSS) vulnerability in the TakeAttendance.php via the cp_id_miss_attn parameter.  CVE ID: CVE-2021-40310	N/A	A-OS4-OPEN- 061021/266
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-21	4.3	OpenSIS Community Edition version <= 7.6 is affected by a reflected XSS vulnerability in EmailCheck.php via the "opt" parameter.  CVE ID: CVE-2021-27340	https://githu b.com/OS4E D/openSIS- Classic/com mit/f78407d 5291c686c3f 416073dcb9 143f3a3d54 89#diff- 24b751f207 2f058259d0 3301693810 1f9fa29884e bcc09ce7eb8 8def3421e5b a	A-OS4-OPEN- 061021/267
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	tricted ectory ath			https://githu b.com/OS4E D/openSIS- Classic/com mit/f78407d 5291c686c3f 416073dcb9 143f3a3d54 89#diff- 24b751f207 2f058259d0 3301693810	A-OS4-OPEN- 061021/268

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1f9fa29884e bcc09ce7eb8 8def3421e5b a	
7				
ve_defense_3	60			
23-Sep-21	4.4	DLL hijacking in Panda Agent <=1.16.11 in Panda Security, S.L.U. Panda Adaptive Defense 360 <= 8.0.17 allows attacker to escalate privileges via maliciously crafted DLL file.  CVE ID: CVE-2021-26750	N/A	A-PAN-PAND- 061021/269
s_agent				
23-Sep-21	4.4	DLL hijacking in Panda Agent <=1.16.11 in Panda Security, S.L.U. Panda Adaptive Defense 360 <= 8.0.17 allows attacker to escalate privileges via maliciously crafted DLL file.  CVE ID : CVE-2021-26750	N/A	A-PAN-PAND- 061021/270
nity				
23-Sep-21	5	Payara Micro Community 5.2021.6 and below allows Directory Traversal.  CVE ID: CVE-2021-41381	https://ww w.payara.fish	A-PAY-MICR- 061021/271
20-Sep-21	6.8	An issue was discovered in pbrt through 20200627. A	N/A	A-PBR-PBRT-
	23-Sep-21 23-Sep-21 23-Sep-21	23-Sep-21 4.4  23-Sep-21 5	DLL hijacking in Panda Agent <=1.16.11 in Panda Security, S.L.U. Panda Adaptive Defense 360 <= 8.0.17 allows attacker to escalate privileges via maliciously crafted DLL file. CVE ID: CVE-2021-26750  Sagent  DLL hijacking in Panda Agent <=1.16.11 in Panda Security, S.L.U. Panda Adaptive Defense 360 <= 8.0.17 allows attacker to escalate privileges via maliciously crafted DLL file. CVE ID: CVE-2021-26750  mity  Payara Micro Community 5.2021.6 and below allows Directory Traversal. CVE ID: CVE-2021-41381	bcc09ce7eb8 8def3421e5b a  Pe_defense_360  23-Sep-21  4.4  DLL hijacking in Panda Agent <=1.16.11 in Panda Security, S.L.U. Panda Adaptive Defense 360 <= 8.0.17 allows attacker to escalate privileges via maliciously crafted DLL file. CVE ID: CVE-2021-26750  Sagent  DLL hijacking in Panda Agent <=1.16.11 in Panda Security, S.L.U. Panda Adaptive Defense 360 <= 8.0.17 allows attacker to escalate privileges via maliciously crafted DLL file. CVE ID: CVE-2021-26750  N/A  payara Micro Community S.2021.6 and below allows Directory Traversal. CVE ID: CVE-2021-41381  https://ww w.payara.fish  An issue was discovered in N/A

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Write			stack-buffer-overflow exist in the function pbrt::ParamSet::ParamSet(located in paramset.h. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-32299		061021/272
pdftools_proj	ect				
pdftools					
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in pdftools through 20200714 A NULL pointer dereference exists in the function node::ObjNode::Value() located in objnode.cpp. It allows an attacker to cause Denial of Service.	4. re N/A	A-PDF-PDFT- 061021/273
			CVE ID: CVE-2021-39538	3	
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in pdftools through 20200714 A NULL pointer dereference exists in the function node::BDCNode::~BDCNod ) located in bdcnode.cpp. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39539	4. le( N/A	A-PDF-PDFT- 061021/274
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in pdftools through 20200714 A stack-buffer-overflow exists in the function Analyze::AnalyzePages() located in analyze.cpp. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-39540	4. N/A	A-PDF-PDFT- 061021/275
NULL Pointer	20-Sep-21	4.3	An issue was discovered in pdftools through 20200714	N/A	A-PDF-PDFT- 061021/276
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-</b> 0		8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Dereference			A NULL pointer dereference exists in the function Analyze::AnalyzeXref() located in analyze.cpp. It allows an attacker to cause Denial of Service.		
			CVE ID : CVE-2021-39541		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function Font::Size() located in font.cpp. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39542	N/A	A-PDF-PDFT- 061021/277
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function Analyze::AnalyzeRoot() located in analyze.cpp. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39543	N/A	A-PDF-PDFT- 061021/278
pi-hole					
web_interface	e				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-21	4.3	adminite is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CVE ID: CVE-2021-3811	https://hunt r.dev/bounti es/fa38c61f- 4043-4872- bc85- 7fe5ae5cc2e 8, https://githu b.com/pi- hole/adminlt e/commit/f5 26716de7bb	A-PIWEB 061021/279

2-3 3-4 4-5

1-2

0-1

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
				0fd382a64bc bbb33915c9 26f94bb			
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-21	4.3	adminite is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CVE ID: CVE-2021-3812	https://hunt r.dev/bounti es/875a688 5-9a64-46f3- 94ad- 92f40f98920 0, https://githu b.com/pi- hole/adminlt e/commit/f5 26716de7bb 0fd382a64bc bbb33915c9 26f94bb	A-PIWEB 061021/280		
Pingidentity							
pingaccess							
Inconsistent Interpretatio n of HTTP Requests ('HTTP Request Smuggling')	24-Sep-21	5	Ping Identity PingAccess before 5.3.3 allows HTTP request smuggling via header manipulation.  CVE ID: CVE-2021-31923	https://docs. pingidentity. com/bundle/ pingaccess- 53/page/wc o162983310 4567.html	A-PIN-PING- 061021/281		
plasticscm							
plastic_scm							
N/A	22-Sep-21	5	Plastic SCM before 10.0.16.5622 mishandles the WebAdmin server management interface.  CVE ID: CVE-2021-41382	https://ww w.plasticscm. com/downlo ad/releaseno tes/10.0.16.5	A-PLA-PLAS- 061021/282		
print_my_blog_project							
print_my_blog	g						

Cross-Site Request Forgery (CSRF)  Realvnc vnc_viewer	20-Sep-21	5.8	The Print My Blog WordPress Plugin before 3.4.2 does not enforce nonce (CSRF) checks, which allows attackers to make logged in administrators deactivate the Print My Blog plugin and delete all saved data for that plugin by tricking them to	N/A	A-PRI-PRIN- 061021/283
			open a malicious link  CVE ID : CVE-2021-24636		332321, 233
vnc_viewer					
Improper Input 17 Validation	17-Sep-21	4.3	** DISPUTED ** RealVNC Viewer 6.21.406 allows remote VNC servers to cause a denial of service (application crash) via crafted RFB protocol data. NOTE: It is asserted that this issue requires social engineering a user into connecting to a fake VNC Server. The VNC Viewer application they are using will then hang, until terminated, but no memory leak occurs - the resources are freed once the hung process is terminated and the resource usage is constant during the hang. Only the process that is connected to the fake Server is affected. This is an application bug, not a security issue.  CVE ID: CVE-2021-41380	N/A	A-REA-VNC 061021/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
revive_adserv	er				
Use of a Broken or Risky Cryptographi c Algorithm	23-Sep-21	4.3	Vulnerability in the generation of session IDs in revive-adserver < 5.3.0, based on the cryptographically insecure uniqid() PHP function. Under some circumstances, an attacker could theoretically be able to brute force session IDs in order to take over a specific account.  CVE ID: CVE-2021-22948	https://ww w.revive- adserver.co m/security/r evive-sa- 2021-005/	A-REV-REVI- 061021/285
schiocco					
support_boar	dchat_and	_help_o	lesk		
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	7.5	The Support Board WordPress plugin before 3.3.4 does not escape multiple POST parameters (such as status_code, department, user_id, conversation_id, conversation_status_code, and recipient_id) before using them in SQL statements, leading to SQL injections which are exploitable by unauthenticated users.  CVE ID: CVE-2021-24741	https://boar d.support/ch anges	A-SCH-SUPP- 061021/286
seatd_project					
seatd					
Improper Privilege Management	17-Sep-21	8.5	seatd-launch in seatd 0.6.x before 0.6.2 allows privilege escalation because it uses execlp and may be installed setuid root.  CVE ID: CVE-2021-41387	N/A	A-SEA-SEAT- 061021/287

2-3 3-4 4-5

1-2

0-1

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pat	ch:	NCI	IPC ID
sela_project										
sela										
Out-of- bounds Write	20-Sep-21	sela th file::W wav_fi buffer	ue was de rough 2  VavFile::vile.c has de overflow  D: CVE-2	020041 writeTo a heap-l w.	2. File() in pased	N/A		_	-SELA- 21/288	
NULL Pointer Dereference	20-Sep-21	4.3	An iss sela th NULL exists rice::R locate allows Denial	An issue was discovered in sela through 20200412. A  NULL pointer dereference exists in the function rice::RiceDecoder::process() located in rice_decoder.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39545					_	-SELA- 21/289
Out-of- bounds Write	20-Sep-21	6.8	sela th rice::R in rice heap-l	ue was de rough 2 RiceDeco e_decode based bu	020041 der::pro r.cpp ha affer ove	2. ocess() as a orflow.	N/A		_	-SELA- 21/290
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function lpc::SampleGenerator::proces s() located in sample_generator.cpp. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39547				N/A			-SELA- 21/291
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function frame::FrameDecoder::proces				N/A			-SELA- 21/292
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			s() located in frame_decoder.c. It allows an attacker to cause Denial of Service.				
			CVE ID: CVE-2021-39548				
NULL Pointer Dereference	20-Sep-21 nce		20-Sep-21 4.3		An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function file::WavFile::WavFile() located in wav_file.c. It allows an attacker to cause Denial of Service.		A-SEL-SELA- 061021/293
			CVE ID: CVE-2021-39549				
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in sela through 20200412. file::SelaFile::readFromFile() in sela_file.cpp has a heapbased buffer overflow.	N/A	A-SEL-SELA- 061021/294		
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in sela through 20200412. file::SelaFile::readFromFile() in sela_file.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39551	N/A	A-SEL-SELA- 061021/295		
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in sela through 20200412. file::WavFile::readFromFile() in wav_file.c has a heap-based buffer overflow.  CVE ID: CVE-2021-39552	N/A	A-SEL-SELA- 061021/296		
set_user_proje	ect						
set_user							
N/A	27-Sep-21	7.5	The set_user extension module before 3.0.0 for PostgreSQL allows	https://githu b.com/pgaud it/set_user/r	A-SET-SET 061021/297		
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID					
			ProcessUtility_hook bypass via set_config.  CVE ID: CVE-2021-41558	eleases/tag/ REL3_0_0						
sharpcompress_project										
sharpcompro	sharpcompress									
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Sep-21	4	SharpCompress is a fully managed C# library to deal with many compression types and formats. Versions prior to 0.29.0 are vulnerable to partial path traversal.  SharpCompress recreates a hierarchy of directories under destinationDirectory if ExtractFullPath is set to true in options. In order to prevent extraction outside the destination directory the destinationFileName path is verified to begin with fullDestinationDirectoryPath. However, prior to version 0.29.0, it is not enforced that fullDestinationDirectoryPath ends with slash. If the destinationDirectory is not slash terminated like '/home/user/dir' it is possible to create a file with a name thats begins as the destination directory one level up from the directory, i.e. '/home/user/dir.sh'. Because of the file name and destination directory constraints the arbitrary file creation impact is limited and depends on the use case. This issue is fixed in SharpCompress version	https://github.com/adamhathcock/sharpcompress/security/advisories/GHSA-jp7f-grcv-6mjf,https://github.com/adamhathcock/sharpcompress/pull/614	A-SHA-SHAR-061021/298					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			0.29.0.						
			CVE ID : CVE-2021-39208						
Siemens	Siemens								
solid_edge	solid_edge								
Out-of- bounds Read	28-Sep-21	4.3	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13565).	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 728618.pdf	A-SIE-SOLI- 061021/299				
			CVE ID : CVE-2021-41533						
Out-of- bounds Read	28-Sep-21	4.3	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing JT files. An attacker could leverage this vulnerability to leak information in the context of the current process (ZDI-CAN-13703).  CVE ID: CVE-2021-41534	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 728618.pdf	A-SIE-SOLI- 061021/300				
Use After Free	28-Sep-21	6.8	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a useafter-free vulnerability while	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 728618.pdf	A-SIE-SOLI- 061021/301				
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 109 of 861	6-7 7-8	8-9 9-10				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13771).  CVE ID: CVE-2021-41535		
Use After Free	28-Sep-21	6.8	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a useafter-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13778).  CVE ID: CVE-2021-41536	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 728618.pdf	A-SIE-SOLI- 061021/302
Use After Free	28-Sep-21	6.8	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a useafter-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13789).  CVE ID: CVE-2021-41537	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 728618.pdf	A-SIE-SOLI- 061021/303
Access of Uninitialized Pointer	28-Sep-21	4.3	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application is vulnerable to information disclosure by unexpected access to an uninitialized pointer while parsing user-supplied OBJ	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 728618.pdf	A-SIE-SOLI- 061021/304
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 110 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			files. An attacker could leverage this vulnerability to leak information from unexpected memory locations (ZDI-CAN-13770).  CVE ID: CVE-2021-41538				
Use After Free	28-Sep-21	6.8	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a useafter-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13773).  CVE ID: CVE-2021-41539	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 728618.pdf	A-SIE-SOLI- 061021/305		
Use After Free	28-Sep-21	6.8	A vulnerability has been identified in Solid Edge SE2021 (All versions < SE2021MP8). The affected application contains a useafter-free vulnerability while parsing OBJ files. An attacker could leverage this vulnerability to execute code in the context of the current process (ZDI-CAN-13776).  CVE ID: CVE-2021-41540	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 728618.pdf	A-SIE-SOLI- 061021/306		
simple_schoo	_ ls_staff_direc	tory_p	roject				
	simple_schools_staff_directory						
Unrestricted Upload of File with Dangerous Type	20-Sep-21	6.5	The Simple Schools Staff Directory WordPress plugin through 1.1 does not validate uploaded logo pictures to ensure that are indeed images, allowing high	N/A	A-SIM-SIMP- 061021/307		

1-2

0-1

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

skale  Sgxwallet  An issue was discovered in SKALE sgxwallet 1.58.3. sgx_disp_ippsAES_GCMEncry pt allows an out-of-bounds write, resulting in a segfault and compromised enclave. This issue describes a buffer overflow, which was resolved prior to v1.77.0 and not reproducible in latest sgxwallet v1.77.0  CVE ID : CVE-2021-36218  An issue was discovered in SKALE sgxwallet 1.58.3. sgx_disp_ippsAES_GCMEncry pt allows an out-of-bounds write, resulting in a segfault and compromised enclave. This issue describes a buffer overflow, which was resolved prior to v1.77.0 and not reproducible in latest sgxwallet v1.77.0  CVE ID : CVE-2021-36218  An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address  A-SKA-1061021							
Skale  Sgxwallet  An issue was discovered in SKALE sgxwallet 1.58.3. sgx_disp_ippsAES_GCMEncry pt allows an out-of-bounds write, resulting in a segfault and compromised enclave. This issue describes a buffer overflow, which was resolved prior to v1.77.0 and not reproducible in latest sgxwallet v1.77.0  CVE ID : CVE-2021-36218  An issue was discovered in SKALE sgxwallet v1.77.0  CVE ID : CVE-2021-36218  An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address  A-SKA-1061021							
Out-of- bounds Write  27-Sep-21  An issue was discovered in SKALE sgxwallet 1.58.3. sgx_disp_ippsAES_GCMEncry pt allows an out-of-bounds write, resulting in a segfault and compromised enclave. This issue describes a buffer overflow, which was resolved prior to v1.77.0 and not reproducible in latest sgxwallet v1.77.0  CVE ID: CVE-2021-36218  An issue was discovered in SKALE sgxwallet v1.77.0  CVE ID: CVE-2021-36218  An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address  27-Sep-21  7.5  An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address  A-SKA-1061021							
An issue was discovered in SKALE sgxwallet 1.58.3. sgx_disp_ippsAES_GCMEncry pt allows an out-of-bounds write, resulting in a segfault and compromised enclave. This issue describes a buffer overflow, which was resolved prior to v1.77.0 and not reproducible in latest sgxwallet v1.77.0  CVE ID: CVE-2021-36218  An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address  An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address  Access of Uninitialized  Pointer							
Out-of- bounds Write  27-Sep-21  A-SKA-Sisgx allet 1.58.3.  Sgx_disp_ippsAES_GCMEncry pt allows an out-of-bounds write, resulting in a segfault and compromised enclave. This issue describes a buffer overflow, which was resolved prior to v1.77.0 and not reproducible in latest sgxwallet v1.77.0  CVE ID: CVE-2021-36218  An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address    https://githu b.com/skale network/sgx wallet/comm it/77425c86 2ad20cd270 d42c54f3d63 e1eb4e0219 5    https://githu b.com/skale network/sgx wallet/comm it/resa a https://githu b.com/skale network/sgx wallet/comm it/4e9b5b75 26db083177							
An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address  An issue was discovered in SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address  A - SKA-5 061021							
SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address  SKALE sgxwallet 1.58.3. The provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized b.com/skale network/sgx wallet/comm it/4e9b5b75 26db083177  A-SKA-State of the provided input for ECALL 14 triggers a branch in trustedEcdsaSign that frees a non-initialized pointer from the stack. An attacker can chain multiple enclave calls to prepare a stack that contains a valid address. This address 26db083177							
is then freed, resulting in compromised integrity of the enclave. This was resolved after v1.58.3 and not reproducible in sgxwallet v1.77.0.  CVE ID: CVE-2021-36219							
solvercircle							
wp_icommerce							
Improper   20-Sep-21   6.5   The Orders functionality in   N/A   A-SOL-	NP_I-						

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')			the WP iCommerce WordPress plugin through 1.1.1 has an `order_id` parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. The feature is available to low privilege users such as contributors CVE ID: CVE-2021-24402		061021/310
speed_test_pr	oject				
speed_test					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Sep-21	5	e7d Speed Test (aka speedtest) 0.5.3 allows a path-traversal attack that results in information disclosure via the "GET /" substring.  CVE ID: CVE-2021-40349	https://old.r eddit.com/r/ HackingTech niques/com ments/poc5 5t/directory_ traversal_by pass_on_e7d_ speedtest/	A-SPE-SPEE- 061021/311
sqlparse_proj	ect			<u> </u>	
sqlparse					
Uncontrolled Resource Consumption	20-Sep-21	5	sqlparse is a non-validating SQL parser module for Python. In sqlparse versions 0.4.0 and 0.4.1 there is a regular Expression Denial of Service in sqlparse vulnerability. The regular expression may cause exponential backtracking on strings containing many repetitions of '\r\n' in SQL comments. Only the formatting feature that removes comments from SQL statements is affected by this	https://githu b.com/andial brecht/sqlpa rse/commit/ 8238a9e450 ed1524e40c b3a8b0b3c0 0606903aeb, https://githu b.com/andial brecht/sqlpa rse/security/ advisories/G HSA-p5w8-	A-SQL-SQLP- 061021/312
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			regular expression. As a workaround don't use the sqlformat.format function with keyword strip_comments=True or thestrip-comments command line flag when using the sqlformat command line tool. The issues has been fixed in sqlparse 0.4.2.  CVE ID: CVE-2021-32839	wqhj-9hhf	
status301					
coolclock					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	3.5	The CoolClock WordPress plugin before 4.3.5 does not escape some shortcode attributes, allowing users with a role as low as Contributor toperform Stored Cross-Site Scripting attacks  CVE ID: CVE-2021-24670	N/A	A-STA-COOL- 061021/313
streama_proj	ect				
streama					
Cross-Site Request Forgery (CSRF)	29-Sep-21	6.8	A cross-site request forgery (CSRF) vulnerability exists in Streama up to and including v1.10.3. The application does not have CSRF checks in place when performing actions such as uploading local files. As a result, attackers could make a logged-in administrator upload arbitrary local files via a CSRF attack and send them to the attacker.  CVE ID: CVE-2021-41764	N/A	A-STR-STRE- 061021/314
stylemixthem	ies				
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ulisting					
Authorizatio n Bypass Through User- Controlled Key	27-Sep-21	6.5	Authenticated Insecure Direct Object References (IDOR) vulnerability in WordPress uListing plugin (versions <= 2.0.5).  CVE ID: CVE-2021-36874	https://word press.org/pl ugins/ulistin g/#develope rs	A-STY-ULIS- 061021/315
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	3.5	Authenticated Reflected Cross-Site Scripting (XSS) vulnerability in WordPress uListing plugin (versions <= 2.0.5). Vulnerable parameters: &filter[id], &filter[user], &filter[expired_date], &filter[created_date], &filter[updated_date].	https://word press.org/pl ugins/ulistin g/#develope rs	A-STY-ULIS- 061021/316
			CVE ID : CVE-2021-36875		
Cross-Site Request Forgery (CSRF)	27-Sep-21	6.8	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in WordPress uListing plugin (versions <= 2.0.5) as it lacks CSRF checks on plugin administration pages.  CVE ID: CVE-2021-36876	https://word press.org/pl ugins/ulistin g/#develope rs	A-STY-ULIS- 061021/317
Cross-Site Request Forgery (CSRF)	27-Sep-21	4.3	Cross-Site Request Forgery (CSRF) vulnerability in WordPress uListing plugin (versions <= 2.0.5) makes it possible for attackers to modify user roles.  CVE ID: CVE-2021-36877	https://word press.org/pl ugins/ulistin g/#develope rs	A-STY-ULIS- 061021/318
Improper Privilege Management	27-Sep-21	7.5	Unauthenticated Privilege Escalation vulnerability in WordPress uListing plugin (versions <= 2.0.5). Possible if WordPress configuration	https://word press.org/pl ugins/ulistin g/#develope rs	A-STY-ULIS- 061021/319

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			allows user registration.		
			CVE ID: CVE-2021-36879		
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	27-Sep-21	7.5	Unauthenticated SQL Injection (SQLi) vulnerability in WordPress uListing plugin (versions <= 2.0.3), vulnerable parameter: custom.  CVE ID: CVE-2021-36880		A-STY-ULIS- 061021/320
surelinesyste	ms				
sureedge_mig	grator				
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-21	7.5	A SQL injection vulnerability exists in Sureline SUREedge Migrator 7.0.7.29360.  CVE ID: CVE-2021-38303	N/A	A-SUR-SURE- 061021/321
Swftools					
swftools					
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function grealloc() located in gmem.cc It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39553	. N/A	A-SWF- SWFT- 061021/322
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function Lexer::Lexer() located in Lexer.cc. It allows an attacker		A-SWF- SWFT- 061021/323
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 <b>9-10</b>

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			to cause Denial of Service.		
			CVE ID : CVE-2021-39554		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function InfoOutputDev::type3D0() located in InfoOutputDev.cc. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39555	N/A	A-SWF- SWFT- 061021/324
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function InfoOutputDev::type3D1() located in InfoOutputDev.cc. It allows an attacker to cause Denial of Service.	N/A	A-SWF- SWFT- 061021/325
			CVE ID: CVE-2021-39556		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function copyString() located in gmem.cc. It allows an attacker to cause Denial of Service.	N/A	A-SWF- SWFT- 061021/326
			CVE ID: CVE-2021-39557		
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function VectorGraphicOutputDev::dra wGeneralImage() located in VectorGraphicOutputDev.cc. It allows an attacker to cause code Execution.	N/A	A-SWF- SWFT- 061021/327

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39558		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function GString::~GString() located in GString.cc. It allows an attacker to cause Denial of Service.	N/A	A-SWF- SWFT- 061021/328
			CVE ID : CVE-2021-39559		
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function Gfx::opSetFillColorN() located in Gfx.cc. It allows an attacker to cause code Execution.	N/A	A-SWF- SWFT- 061021/329
			CVE ID: CVE-2021-39561		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function FileStream::makeSubStream( ) located in Stream.cc. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39562	N/A	A-SWF- SWFT- 061021/330
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_DumpActions() located in swfaction.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39563	N/A	A-SWF- SWFT- 061021/331
Out-of- bounds	20-Sep-21	6.8	An issue was discovered in swftools through 20200710.	N/A	A-SWF- SWFT-

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Write			A heap-buffer-overflow exists in the function swf_DumpActions() located in swfaction.c. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-39564		061021/332
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function OpAdvance() located in swfaction.c. It allows an attacker to cause code Execution.  CVE ID: CVE-2021-39569	N/A	A-SWF- SWFT- 061021/333
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function pool_read() located in pool.c. It allows an attacker to cause code Execution.	N/A	A-SWF- SWFT- 061021/334
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function dump_method() located in abc.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39575	N/A	A-SWF- SWFT- 061021/335
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function main() located in swfdump.c. It allows an attacker to cause code Execution.	N/A	A-SWF- SWFT- 061021/336

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39577		
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function string_hash() located in q.c. It allows an attacker to cause code Execution.	N/A	A-SWF- SWFT- 061021/337
			CVE ID: CVE-2021-39579		
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function swf_GetPlaceObject() located in swfobject.c. It allows an attacker to cause code Execution.	N/A	A-SWF- SWFT- 061021/338
			CVE ID : CVE-2021-39582		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function pool_lookup_string2() located in pool.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39583	N/A	A-SWF- SWFT- 061021/339
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function namespace_set_hash() located in pool.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39584	N/A	A-SWF- SWFT- 061021/340
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference	N/A	A-SWF- SWFT- 061021/341
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description	on & CVE I	D	Pa	tch	NCI	IPC ID
			exists in the fu traits_dump() abc.c. It allows cause Denial c	located i s an attac	ker to				
			CVE ID : CVE-	2021-39	585				
NULL Pointer Dereference	20-Sep-21	4.3	An issue was of swftools through A NULL points exists in the further swf_DumpABO abc.c. It allows cause Denial of CVE ID : CVE-	igh 2020er dereferanction  C() locates an attace of Service	0710. rence ed in ker to	N/A		A-SWI SWFT 06102	
NULL Pointer Dereference	20-Sep-21	4.3	An issue was of swftools through A NULL points exists in the full swf_ReadABC abc.c. It allows cause Denial of	N/A		A-SWI SWFT 06102			
NULL Pointer Dereference	20-Sep-21	4.3	An issue was of swftools through A NULL points exists in the further parse_metada abc.c. It allows cause Denial of CVE ID : CVE-	N/A		A-SWI SWFT 06102			
NULL Pointer Dereference	20-Sep-21	4.3	An issue was of swftools through A NULL points exists in the further params_dump abc.c. It allows cause Denial of CVE ID : CVE-	N/A		A-SWI SWFT 06102			
NULL	20-Sep-21	4.3	An issue was o	discovere	ed in	N/A		A-SWI	7
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIIPC ID
Pointer Dereference			swftools through 20200710.  A NULL pointer dereference exists in the function swf_GetShapeBoundingBox() located in swfshape.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39591			SWFT- 061021/346
			An issue was discovered in			
NULL Pointer Dereference	20-Sep-21	4.3	swftools through 20200710. A NULL pointer dereference exists in the function pool_lookup_uint() located in pool.c. It allows an attacker to cause Denial of Service.	N/A		A-SWF- SWFT- 061021/347
			CVE ID : CVE-2021-39592			
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_FontExtract_DefineFontInfo() located in swftext.c. It allows an attacker to cause Denial of Service.	N/A		A-SWF- SWFT- 061021/348
			CVE ID : CVE-2021-39593			
NULL Pointer Dereference	20-Sep-21	4.3	Other An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function updateusage() located in swftext.c. It allows an attacker to cause Denial of Service.	N/A		A-SWF- SWFT- 061021/349
			CVE ID : CVE-2021-39594			
Out-of- bounds Write	20-Sep-21	6.8	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function rfx_alloc() located in mem.c.	N/A		A-SWF- SWFT- 061021/350
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			It allows an attacker to cause code Execution.  CVE ID: CVE-2021-39595		
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function code_parse() located in code.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39596	N/A	A-SWF- SWFT- 061021/351
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function code_dump2() located in code.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39597	N/A	A-SWF- SWFT- 061021/352
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function callcode() located in code.c. It allows an attacker to cause Denial of Service.  CVE ID: CVE-2021-39598	N/A	A-SWF- SWFT- 061021/353
taro					
taro					,
N/A	17-Sep-21	7.8	taro is vulnerable to Inefficient Regular Expression Complexity CVE ID: CVE-2021-3804	https://hunt r.dev/bounti es/0ebe85e6 -cc85-42b8- 957e- 18d8df2774 14, https://githu b.com/nervjs	A-TAR-TARO- 061021/354
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/taro/commi t/acadb6c82 6ba57f2030a 626f1de4f7b 4608fcdb5	
telefication					
telefication					
Server-Side Request Forgery (SSRF)	22-Sep-21	5	The Telefication WordPress plugin is vulnerable to Open Proxy and Server-Side Request Forgery via the ~/bypass.php file due to a user-supplied URL request value that gets called by a curl requests. This affects versions up to, and including, 1.8.0.  CVE ID: CVE-2021-39339	N/A	A-TEL-TELE- 061021/355
thinktwit_pro	ject				
thinktwit					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The ThinkTwit WordPress plugin before 1.7.1 did not sanitise or escape its "Consumer key" setting before outputting it its settings page, leading to a Stored Cross-Site Scripting issue.  CVE ID: CVE-2021-24582	N/A	A-THI-THIN- 061021/356
Torproject					
tor_browser					
Insertion of Sensitive Information into Log File	24-Sep-21	3.6	Tor Browser through 10.5.6 and 11.x through 11.0a4 allows a correlation attack that can compromise the privacy of visits to v2 onion addresses. Exact timestamps	https://gitla b.torproject. org/tpo/core /tor/- /commit/80 c404c4b79f3	A-TOR-TOR 061021/357

6-7

7-8

8-9

9-10

2-3 3-4 4-5

1-2

0-1

CVSS Scoring Scale

of these onion-service visits are logged locally, and an attacker might be able to compare them to timestamp data collected by the destination server (or collected by a rogue site within the Tor network).  CVE ID : CVE-2021-39246  Trendmicro    Nousecall_for_home_networks	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Search Path Element  A-TRE-HOUS-Object on the target system to exploit this vulnerability.  CVE ID: CVE-2021-32466   A-TRE-HOUS-Object on the target system to exploit this vulnerability.  CVE ID: CVE-2021-32466  ServerProtect for Storage 6.0, ServerProtect for Storage 6.0, ServerProtect for EMC Celerra 5.8, ServerProtect for Network Appliance Filers 5.8, and ServerProtect for Microsoft Windows / Novell Netware 5.8 could allow a remote attacker to bypass  A-TRE-SERV-Object on Network Protect for Microsoft Windows / Novell Netware 5.8 could allow a remote attacker to bypass	Trendmicro			are logged locally, and an attacker might be able to compare them to timestamp data collected by the destination server (or collected by a rogue site within the Tor network).	d4c62a62a0 4f3ed9, https://gitla b.torproject. org/tpo/core /tor/- /merge_requ	
Uncontrolled Search Path Element  A-TRE-HOUS-load a malicious library. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.  CVE ID: CVE-2021-32466  ServerProtect for Storage 6.0, ServerProtect for Storage 6.0	housecall_for	_home_netwo	orks			
Improper Authenticati on  29-Sep-21  A vulnerability in Trend Micro ServerProtect for Storage 6.0, ServerProtect for EMC Celerra 5.8, ServerProtect for Network Appliance Filers 5.8, and ServerProtect for Microsoft Windows / Novell Netware 5.8 could allow a remote attacker to bypass  A-TRE-SERV- 061021/359  attacker to bypass	Search Path	29-Sep-21	6.9	element privilege escalation vulnerability in Trend Micro HouseCall for Home Networks version 5.3.1225 and below could allow an attacker to escalate privileges by placing a custom crafted file in a specific directory to load a malicious library. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	enter.trendm icro.com/ja- jp/article/T MKA-10621, https://helpc enter.trendm icro.com/en- us/article/t	
Improper Authenticati on  On  Micro ServerProtect for Storage 6.0, ServerProtect for EMC Celerra 5.8, ServerProtect for Network Appliance Filers 5.8, and ServerProtect for Microsoft Windows / Novell Netware 5.8 could allow a remote attacker to bypass  Micro ServerProtect for ess.trendmic ro.com/solut ion/0002890 38, https://succ ess.trendmic ro.com/jp/so lution/0002 89030	serverprotect	t .				
	Authenticati	29-Sep-21	10	Micro ServerProtect for Storage 6.0, ServerProtect for EMC Celerra 5.8, ServerProtect for Network Appliance Filers 5.8, and ServerProtect for Microsoft Windows / Novell Netware 5.8 could allow a remote attacker to bypass	ess.trendmic ro.com/solut ion/0002890 38, https://succ ess.trendmic ro.com/jp/so lution/0002	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			installations.							
			CVE ID: CVE-2021-36745							
tubitak										
pardus_softw	pardus_software_center									
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Sep-21	7.1	A path traversal vulnerability on Pardus Software Center's "extractArchive" function could allow anyone on the same network to do a man-in-the-middle and write files on the system.  CVE ID: CVE-2021-3806	https://pent est.blog/par dus-21- linux-distro- remote- code- execution- 0day-2021/, https://ww w.usom.gov.t r/bildirim/tr -21-0754	A-TUB-PARD- 061021/360					
ui										
unifi_talk										
Improper Control of Generation of Code ('Code Injection')	23-Sep-21	6.5	A vulnerability found in UniFi Talk application V1.12.3 and earlier permits a malicious actor who has already gained access to a network to subsequently control Talk device(s) assigned to said network if they are not yet adopted. This vulnerability is fixed in UniFi Talk application V1.12.5 and later.  CVE ID: CVE-2021-22952	N/A	A-UI-UNIF- 061021/361					
Vmware										
cloud_founda	tion									
Server-Side Request Forgery (SSRF)	23-Sep-21	4	The vCenter Server contains an SSRF (Server Side Request Forgery) vulnerability due to improper validation of URLs in vCenter Server Content	https://ww w.vmware.co m/security/a dvisories/V MSA-2021-	A-VMW- CLOU- 061021/362					
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 126 of 861	6-7 7-8	8-9 9-10					

Weakness	Publish Date	cvss	Description	on & CVE ID	Pa	tch	NCI	PC ID
			Library. An automatic with access to may exploit the sending a POST vCenter Server information dicenter CVE ID: CVE-2	content librar is issue by I request to cleading to sclosure.	0020.l	ntml		
Unrestricted Upload of File with Dangerous Type	23-Sep-21	7.5	The vCenter Se an arbitrary fil vulnerability in service. A mali with network a 443 on vCente exploit this iss code on vCente uploading a sp file.	e upload n the Analytic cious actor access to port r Server may ue to execute er Server by ecially crafted	https:/ w.vmv m/sec dvisor MSA-2	vare.co urity/a ies/V 2021-	A-VMV CLOU- 06102	-
			CVE ID : CVE-2 The vCenter Se		2			
N/A	23-Sep-21	5	reverse proxy vulnerability d the endpoints A malicious ac network acces on vCenter Ser exploit this iss restricted endpoints CVE ID : CVE-2	bypass lue to the way handle the UR tor with s to port 443 wer may ue to access points.	https://w.vmv	vare.co urity/a ies/V 2021-	A-VM\ CLOU- 06102	
Exposure of Resource to Wrong Sphere	23-Sep-21	2.1	The vCenter Selocal informativulnerability in service. An autuser with non-privilege may issue to gain acsensitive infor CVE ID: CVE-2	ion disclosure in the Analytic chenticated cadministrative exploit this ccess to mation.	https:/ w.vmv e m/sec dvisor MSA-2	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html		V- 1/365
						A-VMW-		
Exposure of Resource to	23-Sep-21	5	The vCenter Se an information			//ww vare.co	A-VM\ CLOU-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			vulnerability in VAPI (vCenter API) service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue by sending a specially crafted json-rpc message to gain access to sensitive information.  CVE ID: CVE-2021-22008	m/security/a dvisories/V MSA-2021- 0020.html	061021/366
Uncontrolled Resource Consumption	23-Sep-21	5	The vCenter Server contains multiple denial-of-service vulnerabilities in VAPI (vCenter API) service. A malicious actor with network access to port 443 on vCenter Server may exploit these issues to create a denial of service condition due to excessive memory consumption by VAPI service.  CVE ID: CVE-2021-22009	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- CLOU- 061021/367
Uncontrolled Resource Consumption	23-Sep-21	5	The vCenter Server contains a denial-of-service vulnerability in VPXD service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to create a denial of service condition due to excessive memory consumption by VPXD service.  CVE ID: CVE-2021-22010	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- CLOU- 061021/368
N/A	23-Sep-21	5	vCenter Server contains an unauthenticated API endpoint vulnerability in vCenter Server Content Library. A malicious actor	https://ww w.vmware.co m/security/a dvisories/V MSA-2021-	A-VMW- CLOU- 061021/369

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			with network access to port 443 on vCenter Server may exploit this issue to perform unauthenticated VM network setting manipulation.  CVE ID: CVE-2021-22011	0020.html	
Exposure of Resource to Wrong Sphere	23-Sep-21	5	The vCenter Server contains an information disclosure vulnerability due to an unauthenticated appliance management API. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information.  CVE ID: CVE-2021-22012	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- CLOU- 061021/370
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Sep-21	5	The vCenter Server contains a file path traversal vulnerability leading to information disclosure in the appliance management API. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information.  CVE ID: CVE-2021-22013	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- CLOU- 061021/371
N/A	23-Sep-21	9	The vCenter Server contains an authenticated code execution vulnerability in VAMI (Virtual Appliance Management Infrastructure). An authenticated VAMI user with network access to port 5480 on vCenter Server may exploit this issue to execute code on the underlying operating system that hosts	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- CLOU- 061021/372

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')  N/A  23-Sep-21  N/A  23-Sep-21  A.3  The vCenter Server contains a reflected cross-site scripting vulnerability due to a lack of input sanitization. An attacker may exploit this issue to execute malicious scripts by tricking a victim into clicking a malicious link.  CVE ID: CVE-2021-22016  The vCenter Server contains an arbitrary file deletion vulnerability in a VMware vSphere Life-cycle Manager plug-in. A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete non critical files.  CVE ID: CVE-2021-22018  The vCenter Server contains an arbitrary file deletion vulnerability in a VMware vSphere Life-cycle Manager plug-in. A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete non critical files.  CVE ID: CVE-2021-22018  The vCenter Server contains a denial-of-service vulnerability in VAPI (vCenter API) service. A malicious actor with network www.mware.co m/security/a dvisories/V m/SA-2021- 0020.html  A-VMV CLOU-06102  A-VMV MSA-2021- 0020.html  A-VMV MSA-2021- 0020.html	Weakness	Publish Date	cvss		Description	n & CVE	ID	Pa	tch	NCI	PC ID			
Improper Privilege Management  23-Sep-21  7.2  Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')  N/A  23-Sep-21  A-VMI The vCenter Server contains multiple local privilege escalation vulnerabilities due to improper permissions of files and directories. An authenticated local user with non-administrative privilege may exploit these issues to elevate their privileges to root on vCenter Server Appliance.  CVE ID : CVE-2021-22015  The vCenter Server contains a reflected cross-site scripting vulnerability due to a lack of input sanitization. An attacker may exploit this issue to execute malicious scripts by tricking a victim into clicking a malicious link.  CVE ID : CVE-2021-22016  The vCenter Server contains an arbitrary file deletion vulnerability in a Mware vSphere Life-cycle Manager plug-in. A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete non critical files.  CVE ID : CVE-2021-22018  The vCenter Server contains a denial-of-service vulnerability in VAPI (vCenter API) service. A malicious actor with network w.vmware.co m/security/a dvisories/V MSA-2021-0020.html  The vCenter Server contains a denial-of-service vulnerability in VAPI (vCenter API) service. A malicious actor with network w.vmware.co m/security/a dvisories/V dvisories/V MSA-2021-0020.html				vCente	er Servei	·.								
Improper Privilege Management 23-Sep-21 7.2				CVE II	) : CVE-2	2021-22	2014							
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')  A-VM CLOU- of Input During Web Page Generation ('Cross-site Scripting')  A-VM CLOU- of Input During Web Page Generation ('Cross-site Scripting')  The vCenter Server contains a reflected cross-site scripting vulnerability due to a lack of input sanitization. An attacker may exploit this issue to execute malicious scripts by tricking a victim into clicking a malicious link.  CVE ID : CVE-2021-22016  The vCenter Server contains an arbitrary file deletion vulnerability in a VMware vSphere Life-cycle Manager plug-in. A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete non critical files.  CVE ID : CVE-2021-22018  The vCenter Server contains a denial-of-service vulnerability in VAPI (vCenter API) service. A malicious actor with network  A-VM MSA-2021- 0020.html	rivilege	23-Sep-21	multiple local privilege escalation vulnerabilities due to improper permissions of files and directories. An authenticated local user with non-administrative privilege may exploit these issues to elevate their privileges to root on vCenter Server				multiple local privilege escalation vulnerabilities due to improper permissions of files and directories. An authenticated local user with non-administrative privilege may exploit these issues to elevate their privileges to root on vCenter Server				w.vmv m/sec dvisor MSA-2	vare.co urity/a ries/V 2021-	CLOU-	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')  N/A  23-Sep-21  A.3  4.3  4.3  4.3  4.3  4.3  4.3  4.3				CVE II	) : CVE-2	2021-22	2015							
N/A  23-Sep-21  6.4  an arbitrary file deletion vulnerability in a VMware vSphere Life-cycle Manager plug-in. A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete non critical files.  CVE ID: CVE-2021-22018  The vCenter Server contains a denial-of-service vulnerability in VAPI (vCenter API) service. A malicious actor with network  MSA-2021-  A-VMV CLOU- 06102  A-VMV CLOU- 06102  A-VMV CLOU- 06102	Jeutralizatio of Input Ouring Web Page Generation 'Cross-site	23-Sep-21	4.3	reflected cross-site scripting vulnerability due to a lack of input sanitization. An attacker may exploit this issue to execute malicious scripts by tricking a victim into clicking a malicious link.				w.vmv m/sec dvisor MSA-2	vare.co urity/a ries/V 2021-	CLOU-				
N/A  23-Sep-21  The vCenter Server contains a denial-of-service vulnerability in VAPI (vCenter API) service. A malicious actor with network  The vCenter Server contains a denial-of-service w.vmware.co m/security/a dvisories/V MSA-2021-	I/A	23-Sep-21	6.4	an arbitrary file deletion vulnerability in a VMware vSphere Life-cycle Manager plug-in. A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete				w.vmv m/sec dvisor MSA-2	vare.co urity/a ries/V 2021-	CLOU-				
access to port 5480 on  CVSS Scoring Scale				The vCenter Server contains a denial-of-service vulnerability in VAPI (vCenter API) service. A malicious actor with network access to port 5480 on				w.vmv m/sec dvisor MSA-2	vare.co urity/a ries/V 2021-	CLOU- 06102				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			vCenter Server may exploit this issue by sending a specially crafted jsonrpc message to create a denial of service condition.  CVE ID: CVE-2021-22019	0020.html	
N/A	23-Sep-21	2.1	The vCenter Server contains a denial-of-service vulnerability in the Analytics service. Successful exploitation of this issue may allow an attacker to create a denial-of-service condition on vCenter Server.	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- CLOU- 061021/377
			CVE ID : CVE-2021-22020		
vcenter_serve	er				
Server-Side Request Forgery (SSRF)	23-Sep-21	ep-21  The vCenter Server contains an SSRF (Server Side Request Forgery) vulnerability due to improper validation of URLs in vCenter Server Content Library. An authorised user with access to content library may exploit this issue by sending a POST request to vCenter Server leading to information disclosure.		https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/378
			CVE ID : CVE-2021-21993		
Unrestricted Upload of File with Dangerous Type	23-Sep-21	7.5	The vCenter Server contains an arbitrary file upload vulnerability in the Analytics service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to execute code on vCenter Server by uploading a specially crafted file.	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/379

CVSS Scoring Scale

0-1

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22005		
N/A	23-Sep-21	5	The vCenter Server contains a reverse proxy bypass vulnerability due to the way the endpoints handle the URI. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to access restricted endpoints.  CVE ID: CVE-2021-22006	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/380
Exposure of Resource to Wrong Sphere	23-Sep-21	2.1	The vCenter Server contains a local information disclosure vulnerability in the Analytics service. An authenticated user with non-administrative privilege may exploit this issue to gain access to sensitive information.  CVE ID: CVE-2021-22007	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/381
Exposure of Resource to Wrong Sphere	23-Sep-21	5	The vCenter Server contains an information disclosure vulnerability in VAPI (vCenter API) service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue by sending a specially crafted json-rpc message to gain access to sensitive information.  CVE ID: CVE-2021-22008	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/382
Uncontrolled Resource Consumption	23-Sep-21	5	The vCenter Server contains multiple denial-of-service vulnerabilities in VAPI (vCenter API) service. A malicious actor with network access to port 443 on vCenter Server may exploit these	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/383

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pa	tch	NCI	IPC ID
Uncontrolled Resource Consumption	23-Sep-21	5	service excessiconsum CVE ID The vCodenial-vulnera A maliconetwor on vCerexploit	conditive memorphism is considered.  constant the constant is constant in the	erver confice n VPXD stor with sto porture to create to	service. 2009 ntains a service. t 443	m/sec dvisor	vare.co urity/a ies/V	A-VMV VCEN- 06102	
			due to o consum service	excessiv nption l	ce condi ve memo by VPXD <b>2021-2</b> 2	ory	MSA-2 0020.ł			,
N/A	23-Sep-21	5	unauth endpoir vCenter Library with ne 443 on exploit unauth setting	enticate nt vulne r Server v. A mal etwork vCente this iss enticate manipu	erability Contenticious access to Server ue to pe	rin etor o port may rform etwork		vare.co urity/a ies/V 021-	A-VMV VCEN- 06102	
Exposure of Resource to Wrong Sphere	23-Sep-21	5	an information and information and information with the content of	rmation ability denticate ement Avith netres 3 on volution sensition.	erver con discloss lue to arged applicated API. A mark accepter Solitive	ure ance alicious cess to erver to gain		vare.co urity/a ies/V 021-	A-VMV VCEN- 06102	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Description & CVE ID		NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Sep-21	5	The vCenter Server contains a file path traversal vulnerability leading to information disclosure in the appliance management API. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information.  CVE ID: CVE-2021-22013	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/387
N/A	23-Sep-21	9	The vCenter Server contains an authenticated code execution vulnerability in VAMI (Virtual Appliance Management Infrastructure). An authenticated VAMI user with network access to port 5480 on vCenter Server may exploit this issue to execute code on the underlying operating system that hosts vCenter Server.  CVE ID: CVE-2021-22014	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/388
Improper Privilege Management	23-Sep-21	7.2	The vCenter Server contains multiple local privilege escalation vulnerabilities due to improper permissions of files and directories. An authenticated local user with non-administrative privilege may exploit these issues to elevate their privileges to root on vCenter Server Appliance.  CVE ID: CVE-2021-22015	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/389
Improper Neutralizatio n of Input	23-Sep-21	4.3	The vCenter Server contains a reflected cross-site scripting vulnerability due to a lack of	https://ww w.vmware.co m/security/a	A-VMW- VCEN- 061021/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			input sanitization. An attacker may exploit this issue to execute malicious scripts by tricking a victim into clicking a malicious link.  CVE ID: CVE-2021-22016	dvisories/V MSA-2021- 0020.html	
N/A	23-Sep-21	5	Rhttproxy as used in vCenter Server contains a vulnerability due to improper implementation of URI normalization. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to bypass proxy leading to internal endpoints being accessed.  CVE ID: CVE-2021-22017	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/391
N/A	23-Sep-21	6.4	The vCenter Server contains an arbitrary file deletion vulnerability in a VMware vSphere Life-cycle Manager plug-in. A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete non critical files.  CVE ID: CVE-2021-22018	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/392
N/A	23-Sep-21	5	The vCenter Server contains a denial-of-service vulnerability in VAPI (vCenter API) service. A malicious actor with network access to port 5480 on vCenter Server may exploit this issue by sending a specially crafted jsonrpc message to create a denial of service condition.	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/393

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22019		
N/A	23-Sep-21	2.1	The vCenter Server contains a denial-of-service vulnerability in the Analytics service. Successful exploitation of this issue may allow an attacker to create a denial-of-service condition on vCenter Server.  CVE ID: CVE-2021-22020	https://ww w.vmware.co m/security/a dvisories/V MSA-2021- 0020.html	A-VMW- VCEN- 061021/394
wbolt			CVEID: CVE 2021 22020		
donate_with_o	arcode				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The Donate With QRCode WordPress plugin before 1.4.5 does not sanitise or escape its QRCode Image setting, which result into a Stored Cross-Site Scripting (XSS). Furthermore, the plugin also does not have any CSRF and capability checks in place when saving such setting, allowing any authenticated user (as low as subscriber), or unauthenticated user via a CSRF vector to update them and perform such attack.	N/A	A-WBO- DONA- 061021/395
			CVE ID : CVE-2021-24618		
webence					
iq_block_coun	itry				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	23-Sep-21	3.5	Authenticated Persistent Cross-Site Scripting (XSS) vulnerability in WordPress iQ Block Country plugin (versions <= 1.2.11). Vulnerable parameter: &blockcountry_blockmessage	https://word press.org/pl ugins/iq- block- country/#de velopers	A-WEB-IQ_B- 061021/396
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
Scripting')			. CVE ID : CVE-2021-36873			
webpsilon						
responsive_3	d_slider					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The Add new scene functionality in the Responsive 3D Slider WordPress plugin through 1.2 uses an id parameter which is not sanitised, escaped or validated before being inserted to a SQL statement, leading to SQL injection. This is a time based SQLI and in the same function vulnerable parameter is passed twice so if we pass time as 5 seconds it takes 10 seconds to return since the query is ran twice.  CVE ID: CVE-2021-24398	N/A	A-WEB-RESP- 061021/397	
weseek						
growi	T	_				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-21	4.3	Cross-site scripting vulnerability due to the inadequate tag sanitization in GROWI versions v4.2.19 and earlier allows remote attackers to execute an arbitrary script on the web browser of the user who accesses a specially crafted page.  CVE ID: CVE-2021-20829	https://wese ek.co.jp/secu rity/2021/0 9/17/vulner ability/growi -prevent- multiple-xss- addition/	A-WES- GROW- 061021/398	
wordpress_popular_posts_project						
wordpress_p		1				
Improper	23-Sep-21	3.5	Authenticated Persistent	https://githu	A-WOR-	
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') wp-board_pro	oject		Cross-Site Scripting (XSS) vulnerability in WordPress Popular Posts plugin (versions <= 5.3.3). Vulnerable at &widget- wpp[2][post_type].  CVE ID : CVE-2021-36872	b.com/cabre rahector/wo rdpress- popular- posts/blob/ master/chan gelog.md	WORD- 061021/399
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The options.php file of the WP-Board WordPress plugin through 1.1 beta accepts a postid parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. This is a time based SQLI and in the same function vulnerable parameter is passed twice so if we pass time as 5 seconds it takes 10 seconds to return since the query ran twice.  CVE ID: CVE-2021-24404	N/A	A-WPWP-B- 061021/400
wp-domain-r		ect			
wp-domain-re	edirect				,
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The Edit domain functionality in the WP Domain Redirect WordPress plugin through 1.0 has an 'editid' parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.  CVE ID: CVE-2021-24401	N/A	A-WPWP-D- 061021/401
wpagecontact	t_project				
wpagecontact_project wpagecontact					

6-7

8-9

7-8

2-3 3-4 4-5

1-2

0-1

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	6.5	The Orders functionality in the WordPress Page Contact plugin through 1.0 has an order_id parameter which is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. The feature is available to low privilege users such as contributors  CVE ID: CVE-2021-24403	N/A	A-WPA- WPAG- 061021/402
wpdevart					
countdown_a	nd_countup\	_woo	commerce_sales_timer		
Cross-Site Request Forgery (CSRF)	28-Sep-21	6.8	The Countdown and CountUp, WooCommerce Sales Timers WordPress plugin is vulnerable to Cross-Site Request Forgery via the save_theme function found in the ~/includes/admin/coundow n_theme_page.php file due to a missing nonce check which allows attackers to inject arbitrary web scripts, in versions up to and including 1.5.7.  CVE ID: CVE-2021-34636	https://plugi ns.trac.word press.org/ch angeset/260 5523/countd own- wpdevart- extended/tru nk/includes/ admin/coun down_theme _page.php	A-WPD- COUN- 061021/403
wpxpo					
postxguten	berg_blocks_	for_po	st_grid		
Incorrect Authorizatio n	27-Sep-21	4	The PostX – Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10 performs incorrect checks before allowing any logged in user to perform some ajax based requests, allowing any user to modify,	N/A	A-WPX-POST- 061021/404

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delete or add ultp_options values.  CVE ID : CVE-2021-24652		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	3.5	The PostX â€" Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10 allows users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks via the plugin's block.  CVE ID: CVE-2021-24659	N/A	A-WPX-POST- 061021/405
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	3.5	The PostX â€" Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10, with Saved Templates Addon enabled, allows users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks via the plugin's shortcode.  CVE ID: CVE-2021-24660	N/A	A-WPX-POST- 061021/406
Exposure of Sensitive Information to an Unauthorize d Actor	27-Sep-21	3.5	The PostX â€" Gutenberg Blocks for Post Grid WordPress plugin before 2.4.10, with Saved Templates Addon enabled, allows users with Contributor roles or higher to read password- protected or private post contents the user is otherwise unable to read, given the post ID.  CVE ID: CVE-2021-24661	N/A	A-WPX-POST- 061021/407
wp_dialog_pro	oject				
wp_dialog					
Improper	20-Sep-21	3.5	The WP Dialog WordPress	N/A	A-WPWP_D-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')			plugin through 1.2.5.5 does not sanitise and escape some of its settings before outputting them in pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.  CVE ID: CVE-2021-24600		061021/408
wp_mapa_pol	itico_espana	_projec	ct		
wp_mapa_pol	itico_espana				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The WP Mapa Politico Espana WordPress plugin before 3.7.0 does not sanitise or escape some of its settings before outputting them in attributes, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed CVE ID: CVE-2021-24609	N/A	A-WP WP_M- 061021/409
wuzhicms					
wuzhicms					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-21	7.5	SQL Injection vulnerability exists in Wuzhi CMS 4.1.0 via the keywords parameter under the coreframe/app/promote/ad min/index.php file.  CVE ID: CVE-2021-40669	N/A	A-WUZ- WUZH- 061021/410
Improper Neutralizatio n of Special Elements	16-Sep-21	7.5	SQL Injection vulnerability exists in Wuzhi CMS 4.1.0 via the keywords iparameter under the	N/A	A-WUZ- WUZH- 061021/411
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1/1 of 861	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')			/coreframe/app/order/admi n/card.php file. CVE ID: CVE-2021-40670		
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-21	7.5	An SQL injection vulnerability exists in Wuzhi CMS v4.1.0 via the KeyValue parameter in coreframe/app/order/admin/index.php.  CVE ID: CVE-2021-40674	N/A	A-WUZ- WUZH- 061021/412
xfig_project					
fig2dev					
NULL Pointer Dereference	20-Sep-21	4.3	An issue was discovered in fig2dev before 3.2.8 A NULL pointer dereference exists in the function compute_closed_spline() located in trans_spline.c. It allows an attacker to cause Denial of Service. The fixed version of fig2dev is 3.2.8.  CVE ID: CVE-2021-32280	https://sour ceforge.net/ p/mcj/ticket s/107/, https://sour ceforge.net/ p/mcj/fig2de v/ci/f17a3b8 a7d54c1bc5 6ab9251253 1772a0b3ec 991/	A-XFI-FIG2- 061021/413
xss_hunter_ex	kpress_proje	ct			
xss_hunter_ex	kpress				
Improper Authenticati on	17-Sep-21	7.5	XSS Hunter Express before 2021-09-17 does not properly enforce authentication requirements for paths.  CVE ID: CVE-2021-41317	https://githu b.com/mand atoryprogra mmer/xsshu nter- express/com mit/56bb44e d9024849f6 4173f71583	A-XSS-XSS 061021/414
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ecb7d873ba ba0	
yithemes					
yith_mainten	ance_mode				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-21	3.5	Authenticated Stored Cross- Site Scripting (XSS) vulnerability in YITH Maintenance Mode (WordPress plugin) versions <= 1.3.7, vulnerable parameter &yith_maintenance_newslette r_submit_label. Possible even when unfiltered HTML is disallowed by WordPress configuration.  CVE ID: CVE-2021-36841	https://word press.org/pl ugins/yith- maintenance - mode/#deve lopers	A-YIT-YITH- 061021/415
you-shang_pr	oject				
you-shang					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-21	3.5	The You Shang WordPress plugin through 1.0.1 does not escape its qrcode links settings, which result into Stored Cross-Site Scripting issues in frontend posts and the plugins settings page depending on the payload used  CVE ID: CVE-2021-24597	N/A	A-YOU-YOU 061021/416
zeesweb					
splash_heade	r				
Improper Neutralizatio n of Input During Web Page Generation	20-Sep-21	3.5	The Splash Header WordPress plugin before 1.20.8 doesn't sanitise and escape some of its settings while outputting them in the admin dashboard, leading to	N/A	A-ZEE-SPLA- 061021/417

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site			an authenticated Stored		
Scripting')			Cross-Site Scripting issue.		
			CVE ID : CVE-2021-24587		
Zohocorp					
manageengin	e_admanage	r_plus			
Server-Side Request Forgery (SSRF)	21-Sep-21	7.5	ManageEngine ADSelfService Plus before 6112 is vulnerable to SSRF.  CVE ID: CVE-2021-37419	https://pitst op.manageen gine.com/po rtal/en/com munity/topic /adselfservic e-plus-6112- hotfix- release	A-ZOH- MANA- 061021/418
Improper Authenticati on	21-Sep-21	5	ManageEngine ADSelfService Plus before 6112 is vulnerable to mail spoofing.  CVE ID: CVE-2021-37420	https://ww w.manageen gine.com, https://pitst op.manageen gine.com/po rtal/en/com munity/topic /adselfservic e-plus-6112- hotfix- release	A-ZOH- MANA- 061021/419
Improper Privilege Management	21-Sep-21	7.5	ManageEngine ADSelfService Plus before 6112 is vulnerable to domain user account takeover.  CVE ID: CVE-2021-37424	https://ww w.manageen gine.com, https://pitst op.manageen gine.com/po rtal/en/com munity/topic /adselfservic e-plus-6112- hotfix- release	A-ZOH- MANA- 061021/420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	27-Sep-21	7.5	Zoho ManageEngine ADManager Plus before 7111 is vulnerable to unrestricted file which leads to Remote code execution.  CVE ID: CVE-2021-37539	https://ww w.manageen gine.com/pr oducts/ad- manager/rel ease- notes.html#7	A-ZOH- MANA- 061021/421
Improper Authenticati on	21-Sep-21	6.5	ManageEngine ADManager Plus before 7111 has Pre- authentication RCE vulnerabilities.  CVE ID: CVE-2021-37741	https://ww w.manageen gine.com/pr oducts/ad- manager/rel ease- notes.html#7 111, https://ww w.manageen gine.com	A-ZOH- MANA- 061021/422
Unrestricted Upload of File with Dangerous Type	27-Sep-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior is vulnerable to unrestricted file upload, leading to remote code execution.  CVE ID: CVE-2021-37761	https://ww w.manageen gine.com/pr oducts/ad- manager/rel ease- notes.html#7	A-ZOH- MANA- 061021/423
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	22-Sep-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior has a Post- Auth OS command injection vulnerability. CVE ID: CVE-2021-37925	https://ww w.manageen gine.com/pr oducts/ad- manager/rel ease- notes.html#7	A-ZOH- MANA- 061021/424
Improper Authenticati on CVSS Scoring Sca	22-Sep-21	7.5	Zoho ManageEngine ADManager Plus version 7110 and prior allows	https://ww w.manageen gine.com/pr oducts/ad-	A-ZOH- MANA- 061021/425

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID				
			account takeover via SSO.  CVE ID: CVE-2021-37927	manager/rel ease- notes.html#7 111					
ZTE									
axon_30_pro_	message_ser	vice							
N/A	25-Sep-21	4.3	There is an information leak vulnerability in the message service app of a ZTE mobile phone. Due to improper parameter settings, attackers could use this vulnerability to obtain some sensitive information of users by accessing specific pages.  CVE ID: CVE-2021-21742  Hardware		A-ZTE-AXON- 061021/426				
	Hardware								
Cisco									
1100-8p									
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	H-CIS-1100- 061021/427				

6-7

7-8

8-9

9-10

2-3 3-4 4-5

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			the attacker to gain privileges equivalent to the root user.		
			CVE ID : CVE-2021-1419		
1120					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-1120- 061021/428
1160					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-1160- 061021/429
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419		
7600_router					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  CVE ID: CVE-2021-1622	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cbr8-cops-Vc2ZsJSx	H-CIS-7600- 061021/430
aironet_1542	d				

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	H-CIS-AIRO- 061021/431
aironet_1542	i				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	H-CIS-AIRO- 061021/432
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
aironet_1562	d		configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419		
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	H-CIS-AIRO- 061021/433
aironet_1562	e				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-AIRO- 061021/434
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NC	IPC ID
aironet_1562			operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419							
un one - 100 -	-		A vulr	erability	in the S	SSH				
Improper Privilege Management	23-Sep-21	7.2	manag multip (APs) local, a modifi device escala vulner impro opera manag netwo could vulner affecte manag config succes the at	vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this			cisco.c curity/ /conte	rityAd /cisco- o-ap-		-AIRO- 21/435
aironet_1815	i									
Improper Privilege Management	23-Sep-21	7.2	mana	A vulnerability in the SSH management feature of multiple Cisco Access Points			cisco.c	//tools. om/se /center		-AIRO- 21/436
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	/content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	
aironet_1815	m				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-AIRO- 061021/437

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			equivalent to the root user.		
			CVE ID : CVE-2021-1419		
aironet_1815	t			<u> </u>	
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-AIRO- 061021/438
aironet_1815	<b>w</b>				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-AIRO- 061021/439
CVSS Scoring Sc	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419		
aironet_1830	e				
Improper Privilege Management	23-Sep-21 7.2		A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	H-CIS-AIRO- 061021/440
aironet_1830					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco-	H-CIS-AIRO- 061021/441
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	sa-cisco-ap- LLjsGxv	
aironet_1840	i		CVEID. GVE-2021-1417		
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-AIRO- 061021/442

0-1

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
aironet_1850	e									
Improper Privilege Management	23-Sep-21	7.2	managemultipe (APs) local, a modification operate management of the attention of the attention operate management of the attention operate	perability gement for platform authenti y files or e and pos ted priv rability i per chec tions wit gement i prk admi exploit t rability b ed device gement t guration ssful exp tacker to alent to t D: CVE-	eature of Access	of Points allow a er to ected in he file SSH A r user sing an h SSH a A d allow ivileges user.	cisco.c curity/ /conte	•		AIRO- 1/443
aironet_1850	i									
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH			cisco.c curity/ /conte	-		AIRO- 1/444	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
aironet_2800e	e		management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419		
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-AIRO- 061021/445
aironet_2800i	i				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-AIRO- 061021/446
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pat	tch	NCI	IPC ID
			improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419							
aironet_3800	e									
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419			https:/ cisco.cc curity/ /conte coSecu visory/ sa-cisc LLjsGx	om/se /center nt/Cis rityAd /cisco- o-ap-	H-CIS- 06102	-AIRO- 21/447	
Improper	Improper 23-Sep-21 7.2 A vulnerability in the SSH https://to					-		-AIRO-		
Privilege  CVSS Scoring Sca	le <b>0-1</b>	1-2	manage	ement f	eature o	of 5-6	cisco.c	om/se 7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Management			multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	
aironet_3800	p				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-AIRO- 061021/449
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			the attacker to gain privileges		
			equivalent to the root user.		
1.000			CVE ID : CVE-2021-1419		
aironet_4800					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	H-CIS-AIRO- 061021/450
asr_1000-x					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa- iosxesdwan- arbfileov- MVOF3ZZn	H-CIS-ASR 061021/451
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723							
asr_1001										
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ASR 061021/452					
asr_1001-x										
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd	H-CIS-ASR 061021/453					
CVSS Scoring Sca	le 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10					

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.	visory/cisco- sa- iosxesdwan- arbfileov- MVOF3ZZn	
asr_1002			CVE ID : CVE-2021-34723		
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa- iosxesdwan- arbfileov- MVOF3ZZn	H-CIS-ASR 061021/454
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
asr_1002-x										
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723				cisco.c curity/ /conte	ov-	H-CIS- 06102	·ASR 21/455
asr_1004										
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful			cisco.c curity/ /conte	ov-	H-CIS- 06102	·ASR 21/456	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
4006			exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723		
asr_1006				l .	l
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosaiosxesdwanarbfileov-MVOF3ZZn	H-CIS-ASR 061021/457
asr_1013					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-iosxesdwan-arbfileov-	H-CIS-ASR 061021/458
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 <b>9-10</b>

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	tch	NCI	IPC ID
			insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723			MVOF3	3ZZn			
asr_1023										
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723			https:/cisco.cc curity/ /conte coSecu visory/ sa- iosxeso arbfile MVOF3	om/se center nt/Cis rityAd cisco- dwan-	H-CIS- 06102	-ASR 21/459	
asr_901-12c-f Improper	23-Sep-21	4.3	A vuln	A vulnerability in the			https:/	/tools.		-ASR
Locking  CVSS Scoring Sca		1-2	Comm	on Oper	Policy	Service 5-6	cisco.co	om/se	06102 8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  CVE ID: CVE-2021-1622	curity/center /content/Cis coSecurityAd visory/cisco- sa-cbr8- cops- Vc2ZsJSx	
asr_901-12c-1	ft-d				
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cbr8- cops- Vc2ZsJSx	H-CIS-ASR 061021/461
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  CVE ID : CVE-2021-1622  A vulnerability in the Common Open Policy Service (COPS) of cisco IoS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets under certain conditions. An attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  H-CIS-ASR061021/462	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Locking  23-Sep-21  4.3  A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a				exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.		
Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a	asr_901-4c-f-	d				
	• •	23-Sep-21	4.3	Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a	cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cbr8- cops-	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1622		
asr_901-4c-ft	-d				
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  CVE ID: CVE-2021-1622	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cbr8-cops-Vc2ZsJSx	H-CIS-ASR 061021/463
asr_901-6cz-1	<u> </u> f-a				
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cbr8- cops- Vc2ZsJSx	H-CIS-ASR 061021/464
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS. CVE ID: CVE-2021-1622    A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker coul exploit this vulnerability sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Locking  23-Sep-21  A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to				condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a		
Improper Locking  23-Sep-21  A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to		_		CVE ID : CVE-2021-1622		
Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to	asr_901-6cz-f	-d				
		23-Sep-21	4.3	Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to	cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cbr8- cops-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  CVE ID: CVE-2021-1622		
asr_901-6cz-fs	s-a		CVLID : CVL 2021 1022		
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  CVE ID: CVE-2021-1622	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cbr8-cops-Vc2ZsJSx	H-CIS-ASR 061021/466
asr_901-6cz-fs	s-d				
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8	https://tools. cisco.com/se curity/center /content/Cis	H-CIS-ASR 061021/467
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 170 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  CVE ID: CVE-2021-1622	coSecurityAd visory/cisco- sa-cbr8- cops- Vc2ZsJSx	
asr_901-6cz-f	ft-a				
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cbr8- cops- Vc2ZsJSx	H-CIS-ASR 061021/468
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  CVE ID: CVE-2021-1622		
asr_901-6cz-1	rt-d				
Improper	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  CVE ID: CVE-2021-1622	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cbr8-cops-Vc2ZsJSx	H-CIS-ASR 061021/469

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
catalyst_9105										
Uncontrolled Resource Consumption	23-Sep-21	5	procest Cisco I Control for Car (APs) unautil attack service affected vulner insuffit An att vulner crafted devices could exhau and car affected traffic	terability ssing fur Embedd oller (EV talyst Accould all henticate (DoS) (ed AP. The ability is acker contability by the acker contability by the stavailanuse a Doctor (EVE-) of the contability of the stavailanuse and the contability of the stavailanuse and the contability of the contability of the stavailanuse and the contability of	nctionali ed Wire VC) Soft ccess Poi low an ed, remo use a der conditio nis s due to ffer allo uld expl oy sendin to an aff essful ex e attack ble reso oS condi , as well for clier ng the A	ty of less ware ints ote nial of n on an cation. oit this ng fected cploit er to urces tion on as a nt AP.	cisco.c curity/ /conte	/center ent/Cis arityAd /cisco- ce- os-		CATA- 1/470
catalyst_9105	axi									
Improper Privilege Management	23-Sep-21	7.2	manag multip (APs) local, a modifi device escala vulner impro operat manag netwo could	gement fole Cisco platform authenti y files or e and post ted priverability i per chece tions with gement i ork admi exploit t	eature of Access	Points allow a ser to ected in he file SSH a. A r user	cisco.c curity/ /conte	/center ent/Cis arityAd /cisco- eo-ap-		CATA- 1/471
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
catalyst_9105  Improper Privilege Management		7.2	affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419  A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	H-CIS-CATA-061021/472
			the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419		
catalyst_9115					
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-iosxe- ewc-dos-	H-CIS-CATA- 061021/473
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 Page 174 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP.	g6JruHRT	
catalyst_9115a	xe				
Improper Privilege Management  catalyst_9115a	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-CATA- 061021/474
. 1 . 0445	***			•	

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-CATA- 061021/475
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-iosxe- ewc-dos- g6JruHRT	H-CIS-CATA- 061021/476
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Catalyst_9117  Improper Privilege Management		7.2	exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP.  CVE ID: CVE-2021-1615  A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco-	H-CIS-CATA- 061021/477
			could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	sa-cisco-ap- LLjsGxv	
catalyst_9120				1	
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-iosxe- ewc-dos- g6JruHRT	H-CIS-CATA- 061021/478
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP.  CVE ID: CVE-2021-1615		
catalyst_9120	axe				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-CATA- 061021/479
catalyst_9120	axi				
Improper	23-Sep-21	7.2	A vulnerability in the SSH	https://tools.	H-CIS-CATA-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	061021/480
catalyst_9120	l Daxp				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-CATA- 061021/481
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419		
catalyst_9124	•				
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP.  CVE ID: CVE-2021-1615	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-iosxe- ewc-dos- g6JruHRT	H-CIS-CATA- 061021/482
catalyst_9124	axd				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-CATA- 061021/483
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 180 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description	n & CVE ID	Patch	NCIIPC ID
catalyst_9124	·axi		operations with management in network admin could exploit th vulnerability by affected device management to configuration cl successful exploit the attacker to gequivalent to the CVE ID: CVE-20	istrator user istrator user is accessing an through SSH make a hange. A oit could allow gain privileges he root user.		
			A vulnerability management fe	ature of		
Improper Privilege Management	23-Sep-21	7.2	multiple Cisco A (APs) platforms local, authentica modify files on device and poss escalated privile vulnerability is improper check operations with management in network admin could exploit th vulnerability by affected device management to configuration cl successful explo the attacker to g equivalent to th  CVE ID: CVE-20	s could allow a ated user to the affected sibly gain eges. The due to king on file nin the SSH aterface. A istrator user as accessing an through SSH o make a hange. A poit could allow gain privileges are root user.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	H-CIS-CATA-
catalyst_9130	)					
Uncontrolled Resource Consumption	23-Sep-21	5	A vulnerability in the packet processing functionality of Cisco Embedded Wireless		https://tools. cisco.com/se curity/center	061021/485
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4	4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Controller (EWC) Software for Catalyst Access Points (APs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected AP. This vulnerability is due to insufficient buffer allocation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to exhaust available resources and cause a DoS condition on an affected AP, as well as a DoS condition for client traffic traversing the AP.	/content/Cis coSecurityAd visory/cisco- sa-iosxe- ewc-dos- g6JruHRT	
catalyst_9130	axe				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-CATA- 061021/486
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID				
			the attacker to gain privileges equivalent to the root user.						
			CVE ID : CVE-2021-1419						
catalyst_9130	catalyst_9130axi								
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-CATA- 061021/487				
catalyst_9800	)- <b>4</b> 0								
Improper Privilege 23-Sep-21 7 Management		7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-CATA- 061021/488				
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10				

30		network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419  A vulnerability in the SSH		
30		_		
		_		
23-Sep-21	7.2	management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-CATA- 061021/489
-1				
23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd	H-CIS-CATA- 061021/490
cl		3-Sep-21 7.2	network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419  A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a	network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419  A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a cosecurityAd visory/cisco-sa-cisco-ap-LLjsGxv  LLjsGxv  https://tools.cisco.com/se curity/center /content/Cis

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.	visory/cisco- sa-cisco-ap- LLjsGxv	
catalyst_9800	<b>)-1</b>		CVE ID : CVE-2021-1419		
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-CATA- 061021/491
CVSS Scoring Sca	ile <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
catalyst_iw63	00_ac									
Improper Privilege Management	23-Sep-21	7.2	management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419			cisco.c curity/ /conte	•		CATA- 21/492	
catalyst_iw63	00_dc									
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH			cisco.c curity/ /conte	-		CATA- 21/493	
CVSS Scoring Sca	ile <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
catalyst_iw63  Improper Privilege Management		7.2	management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419  A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco-	H-CIS-CATA- 061021/494
			could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	sa-cisco-ap- LLjsGxv	
cbr-8					
Improper Locking	23-Sep-21	4.3	A vulnerability in the Common Open Policy Service (COPS) of Cisco IOS XE Software for Cisco cBR-8 Converged Broadband Routers could allow an unauthenticated, remote attacker to cause resource exhaustion, resulting in a	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cbr8- cops- Vc2ZsJSx	H-CIS-CBR 061021/495
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition. This vulnerability is due to a deadlock condition in the code when processing COPS packets under certain conditions. An attacker could exploit this vulnerability by sending COPS packets with high burst rates to an affected device. A successful exploit could allow the attacker to cause the CPU to consume excessive resources, which prevents other control plane processes from obtaining resources and results in a DoS.  CVE ID: CVE-2021-1622		
csr1000v			0.2.2.0.2.2021		
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa- iosxesdwan- arbfileov- MVOF3ZZn	H-CIS-CSR1- 061021/496

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34723		
esw-6300					
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	H-CIS-ESW 061021/497
			A vulnerability in a specific		
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa- iosxesdwan- arbfileov- MVOF3ZZn	H-CIS-ISR1- 061021/498

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723		
isr1100-4g					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa- iosxesdwan- arbfileov- MVOF3ZZn	H-CIS-ISR1- 061021/499
1 4400 4 1			CVE ID : CVE-2021-34723		
isr1100-4glte	ego			I ,	
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-	H-CIS-ISR1- 061021/500
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.	iosxesdwan- arbfileov- MVOF3ZZn	
isr1100-4glter	1a		CVE ID : CVE-2021-34723		
Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ISR1- 061021/501
isr1100-6g					

CVSS Scoring Scale

0-1

5-6

7-8

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
isr_4321  Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723  A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ISR 061021/504
1001			CVE ID : CVE-2021-34723		
isr_4331				latters / // 1	
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa- iosxesdwan- arbfileov- MVOF3ZZn	H-CIS-ISR 061021/505
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723		
isr_4351					
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-iosxesdwan-arbfileov-MVOF3ZZn	H-CIS-ISR 061021/506
isr_4431					
Exposure of Resource to Wrong	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN	https://tools. cisco.com/se curity/center	H-CIS-ISR 061021/507
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723	/content/Cis coSecurityAd visory/cisco- sa- iosxesdwan- arbfileov- MVOF3ZZn	
vedge_100					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX	H-CIS-VEDG- 061021/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vedge_1000					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-sd-wan-Fhqh8pKX	H-CIS-VEDG- 061021/509
vedge_100b					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX	H-CIS-VEDG- 061021/510

6-7

7-8

8-9

9-10

2-3 3-4 4-5

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1546		
vedge_100m					
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX	H-CIS-VEDG- 061021/511
vedge_100wn	n				
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX	H-CIS-VEDG- 061021/512

6-7

7-8

8-9

9-10

2-3 3-4 4-5

1-2

0-1

CVSS Scoring Scale

Containing Sensitive Information  23-Sep-21 2.1 Vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546   Vedge_5000   A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability by running a CLI command that targets an arbitrary file on the disclosure of sensitive information.    Vedge_5000				sensitive information.		
A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability by running a CLI command that targets an arbitrary file, possibly resulting in the disclosure of sensitive information. This vulnerability in the CLI of Cisco SD-WAN Software could exploit this vulnerability by running a CLI command that targets an arbitrary file, possibly resulting in the disclosure of sensitive information.  Vedge_5000   A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information.  Cye ID : CVE-2021-1546   A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to				CVE ID : CVE-2021-1546		
Generation of Error Message Containing Sensitive Information  Generation of Error  Message Containing Sensitive Information  Generation of Error  Message Containing Sensitive Information  Z3-Sep-21  A vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546   A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information.  Generation of Error  Message Containing Sensitive Information  23-Sep-21  23-Sep-21  23-Sep-21  A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to	vedge_2000					
A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to	of Error Message Containing Sensitive	23-Sep-21	2.1	Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.	cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan-	H-CIS-VEDG- 061021/513
Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to	vedge_5000				l	l .
return portions of an arbitrary file, possibly	of Error Message Containing Sensitive	23-Sep-21	2.1	Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an	cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan-	H-CIS-VEDG- 061021/514

resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546   A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546   A vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546   VSMAT Controller  A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An access throu	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
CVE ID : CVE-2021-1546    Vedge_cloud				_		
Generation of Error Message Containing Sensitive Information  Generation of Error Message Containing Sensitive Information  23-Sep-21  2.1  A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546   Vsmart_controller  A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI An excess through the C						
A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID : CVE-2021-1546   VSMAT_CONTOULE   A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file, possibly resulting in the disclosure of sensitive information. This vulnerability is the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through the CLI An improper protections on file access through th				CVE ID : CVE-2021-1546		
Generation of Error Message Containing Sensitive Information  23-Sep-21  23-Sep-21  23-Sep-21  23-Sep-21  23-Sep-21  24  25  Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546   A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file wulnerability is due to improper protections on file improper protections on file // content/Cis // content/Cis // cosecutityAd visory/cisco-sa-sd-wan-Fhqh8pKX  H-CIS-VEDG-061021/515	vedge_cloud	T	T.			
A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI Ap  23-Sep-21  24  A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, https://tools. cisco.com/se curity/center /content/Cis H-CIS-VSMA-	of Error Message Containing Sensitive	23-Sep-21	2.1	Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.	cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan-	
Generation of Error Message  Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLL Ap	vsmart_contr	oller				
Sensitive Information  Informat	of Error Message Containing Sensitive	23-Sep-21	2.1	Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to	cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan-	H-CIS-VSMA- 061021/516

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			arbitrary file, possibly resulting in the disclosure of sensitive information.		
			CVE ID : CVE-2021-1546		
D-link					
dcs-50001					
Improper Authenticati on	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** DCS-5000L v1.05 and DCS-932L v2.17 and older are affecged by Incorrect Acess Control. The use of the basic authentication for the devices command interface allows attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	https://ww w.dlink.com/ en/security- bulletin/, https://supp ortannounce ment.us.dlin k.com/annou ncement/pu blication.asp x?name=SAP 10247	H-D-L-DCS 061021/517
Improper Privilege Management	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** An Elevated Privileges issue exists in D- Link DCS-5000L v1.05 and DCS-932L v2.17 and older. The use of the digest- authentication for the devices command interface may allow further attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the	https://www.dlink.com/en/security-bulletin/,https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10247	H-D-L-DCS 061021/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			maintainer.		
			CVE ID : CVE-2021-41504		
dcs-932l					
Improper Authenticati on	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** DCS-5000L v1.05 and DCS-932L v2.17 and older are affecged by Incorrect Acess Control. The use of the basic authentication for the devices command interface allows attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.  CVE ID: CVE-2021-41503	https://ww w.dlink.com/ en/security- bulletin/, https://supp ortannounce ment.us.dlin k.com/annou ncement/pu blication.asp x?name=SAP 10247	H-D-L-DCS 061021/519
Improper Privilege Management	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** An Elevated Privileges issue exists in D- Link DCS-5000L v1.05 and DCS-932L v2.17 and older. The use of the digest- authentication for the devices command interface may allow further attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.  CVE ID: CVE-2021-41504	https://ww w.dlink.com/ en/security- bulletin/, https://supp ortannounce ment.us.dlin k.com/annou ncement/pu blication.asp x?name=SAP 10247	H-D-L-DCS 061021/520
Dlink			3.2.2.3.2.2.3.1		
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

dir-3040 Use of Hard-			An information disclosure vulnerability exists in the				
Use of Hard-					1		
coded Z Credentials	23-Sep-21	7.5	WiFi Smart Mesh functionality of D-LINK DIR-3040 1.13B03. A specially-crafted network request can lead to command execution. An attacker can connect to the MQTT service to trigger this vulnerability.  CVE ID: CVE-2021-21913	N/A	H-DLI-DIR 061021/521		
dir-605l							
Insufficiently Protected Credentials	24-Sep-21	5	An informtion disclosure issue exists in D-LINK-DIR-605 B2 Firmware Version: 2.01MT. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page  CVE ID: CVE-2021-40655	https://ww w.dlink.com/ en/security- bulletin/	H-DLI-DIR 061021/522		
dir-615							
Insufficiently Protected 2 Credentials	24-Sep-21	4	An information disclosure issue exist in D-LINK-DIR-615 B2 2.01mt. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page  CVE ID: CVE-2021-40654	https://ww w.dlink.com/ en/security- bulletin/	H-DLI-DIR 061021/523		
kadenvodomery							
picoflux_air							
Observable Discrepancy	16-Sep-21	3.3	In Kaden PICOFLUX Air in all known versions an information exposure through observable	https://ww w.fit.vutbr.cz /~polcak/CV E-2021-	H-KAD-PICO- 061021/524		

1-2

0-1

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			discrepancy exists. This may give sensitive information (water consumption without distinct values) to third parties.  CVE ID: CVE-2021-34576	34576.en	
mediatek					
mt6580					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/525
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/526
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/527

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/528
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/529
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/530

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810.		
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/531
			CVE ID : CVE-2021-0612		
mt6582e			<b>Y</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/532
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/533

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/534
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/535
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/536
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp. mediatek.co m/product-	H-MED- MT65- 061021/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilegoral with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	e security- bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp	H-MED- MT65- 061021/538
			CVE ID : CVE-2021-0612		
mt6582h					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp.	H-MED- MT65- 061021/539
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	security- bulletin/Sept	H-MED- MT65- 061021/540
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/541
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/542
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/543

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Use After Free  27-Sep-21  4.6  Use After Free  27-Sep-21  Use After Free  27-Sep-21  Use After Free  Use After Free  Use After Free  27-Sep-21  ALPS05403499; Issue ID: ALPS0	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free  27-Sep-21  4.6  Use After Free  27-Sep-21  4.6  Use After Free  4.6  Use Interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834. CVE ID: CVE-2021-0612  Ale Discussion  Ale Discu				ALPS05411456.		
Use After Free 27-Sep-21 4.6 vith System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611 lttps://corp. mediatek.co m/product-security-bulletin/Sept ember-2021 lttps://corp. mediatek.co m/product-				CVE ID : CVE-2021-0610		
Use After Free  27-Sep-21  4.6  Improper Restriction of Operations within the Bounds of a Memory Buffer  27-Sep-21  A.6  Buse after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834. CVE ID: CVE-2021-0612  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05381071. CVE ID: CVE-2021-0422  H-MED-MT65- 061021/546		27-Sep-21	4.6	memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	mediatek.co m/product- security- bulletin/Sept	MT65-
Improper Restriction of Operations within the Bounds of a Memory Buffer  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05381071.  CVE ID: CVE-2021-0422  In memory management driver, there is a possible system crash due to a missing https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021		27-Sep-21	4.6	memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	mediatek.co m/product- security- bulletin/Sept	MT65-
Improper Restriction of Operations within the Bounds of a Memory Buffer  Odiver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05381071.  CVE ID: CVE-2021-0422   driver, there is a possible system crash due to a missing https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021  H-MED- MT65- 061021/546	mt6582t					
Missing 27-Sep-21 2.1 In memory management https://corp. H-MED-	Restriction of Operations within the Bounds of a Memory	27-Sep-21	2.1	driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	mediatek.co m/product- security- bulletin/Sept	MT65-
	Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	mediatek.co m/product- security- bulletin/Sept ember-2021	MT65- 061021/547
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/548
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/549
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp. mediatek.co m/product- security-	H-MED- MT65- 061021/550
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 210 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	bulletin/Sept ember-2021					
			CVE ID : CVE-2021-0610						
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/551				
			CVE ID : CVE-2021-0611						
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/552				
mt6582w	mt6582w								
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/553				
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

		The state of the s		
		exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.		
		CVE ID : CVE-2021-0422		
27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/554
		CVE ID: CVE-2021-0423		
27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/555
27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/556
	27-Sep-21	27-Sep-21 2.1 27-Sep-21 2.1	27-Sep-21  2.1  In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424  In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05400459.	27-Sep-21  2.1  27-Sep-21  2.1  2.1  2.1  2.1  2.1  2.1  2.1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/557
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/558
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/559
mt6582_90					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp. mediatek.co	H-MED- MT65-

1-2

0-1

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	m/product- security- bulletin/Sept ember-2021	061021/560
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/561
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/562
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp. mediatek.co m/product- security- bulletin/Sept	H-MED- MT65- 061021/563

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/564
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/565
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/566

1-2

0-1

CVSS Scoring Scale

5-6

6-7

8-9

9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834.		
			CVE ID : CVE-2021-0612		
mt6589					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/567
			CVE ID : CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/568
			CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/569

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/570
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/571
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/572
				https://som	H-MED-
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp. mediatek.co m/product-	MT65- 061021/573
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descri	ption & CVE	ID	Pa	itch	NCII	PC ID
			to local esca with System privileges n interaction exploitation ALPS05403 ALPS05425	n execution eeded. Use is not need n. Patch ID: 499; Issue 834.	n er led for ID:		ty- in/Sept 2021		
mt6589td									
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory driver, ther system crass bounds che to local den no addition privileges ninteraction exploitation ALPS05403 ALPS05381	e is a possion due to a ck. This co ial of service eeded. Use is not need a. Patch ID: 499; Issue 071.	ble missing uld lead ce with on er led for	media m/pro securi bulleti	oduct-	H-MEI MT65- 06102	
Missing Initialization of Resource	27-Sep-21	2.1	In memory driver, ther information uninitialize lead to loca disclosure vexecution puser interaction in the second of the second	e is a possing disclosured data. This information with no addition is not exploitation 403499; Is 714.	ble e due to s could on ditional eeded. n. Patch sue ID:	media m/pro securi bulleti	oduct-	H-MEI MT65- 06102	
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory driver, ther system crass bounds che to local den no addition	e is a possich due to a ck. This co ial of servial executio	ble missing uld lead ce with	media m/pro securi bulleti	oduct-	H-MEI MT65- 06102	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/577
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/578
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/579

1-2

0-1

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810.		
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/580
			CVE ID : CVE-2021-0612		
mt6592e					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/581
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/582

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Improper Restriction of Operations within the			In memory management driver, there is a possible system crash due to a missing		
Bounds of a Memory Buffer	27-Sep-21	2.1	bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/583
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/584
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/585
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp. mediatek.co m/product-	H-MED- MT65- 061021/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	security- bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/587
			CVE ID : CVE-2021-0612		
mt6592h					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/588
			CVE ID : CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/589

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/590
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/591
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/592

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456.		
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/593
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/594
mt6592t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/595
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-
CVSS Scoring Sca	ile 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	mediatek.co m/product- security- bulletin/Sept ember-2021	MT65- 061021/596
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/597
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/598
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp. mediatek.co m/product- security-	H-MED- MT65- 061021/599
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 225 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/600
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/601
mt6592w					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/602
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

		exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	-	
		CVE ID : CVE-2021-0422		
27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/603
		CVE ID: CVE-2021-0423		
27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/604
27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/605
	27-Sep-21	27-Sep-21 2.1 27-Sep-21 2.1	driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424  In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05400059.	driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424  In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05400059.

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/606
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/607
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/608
mt6592_90					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp. mediatek.co	H-MED- MT65-

CVSS Scoring Scale

0-1

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	m/product- security- bulletin/Sept ember-2021	061021/609
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/610
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/611
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp. mediatek.co m/product- security- bulletin/Sept	H-MED- MT65- 061021/612

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/613
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/614
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/615

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834.		
			CVE ID : CVE-2021-0612		
mt6595					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/616
			CVE ID : CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/617
			CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/618

6-7

8-9

9-10

7-8

1-2

0-1

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/619
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/620
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT65- 061021/621
				https://sor-	H-MED-
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp. mediatek.co m/product-	MT65- 061021/622
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privile with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	bulletin/Sept ember-2021	
mt6731			CVE ID : CVE-2021-0612		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missi bounds check. This could le to local denial of service wino additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security-	H-MED- MT67- 061021/623
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due uninitialized data. This coullead to local information disclosure with no addition execution privileges needed User interaction is not needed for exploitation. Pat ID: ALPS05403499; Issue II ALPS05385714.	https://corp. mediatek.co mal m/product- security- bulletin/Sept tch ember-2021	H-MED- MT67- 061021/624
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missi bounds check. This could le to local denial of service wi no additional execution  2-3 3-4 4-5 5-6	th security-bulletin/Sept ember-2021	H-MED- MT67- 061021/625

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/626
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/627
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/628

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810.		
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/629
mt6722			CVE ID : CVE-2021-0612		
mt6732			Y		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/630
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/631

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Bounds of a Memory	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp. mediatek.co m/product- security-	H-MED- MT67-
Buffer			exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. CVE ID: CVE-2021-0424	bulletin/Sept ember-2021	061021/632
N/A 2	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/633
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/634
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp. mediatek.co m/product-	H-MED- MT67- 061021/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilegoral with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp	H-MED- MT67- 061021/636
			CVE ID : CVE-2021-0612		
mt6735					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp.	H-MED- MT67- 061021/637
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	security- bulletin/Sept	H-MED- MT67- 061021/638
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/639
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/640
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/641

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456.		
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/642
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/643
mt6737					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/644
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-
CVSS Scoring Sca	le 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	mediatek.co m/product- security- bulletin/Sept ember-2021	MT67- 061021/645
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/646
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/647
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp. mediatek.co m/product- security-	H-MED- MT67- 061021/648

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/649
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/650
mt6739					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/651
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.		
		CVE ID : CVE-2021-0422		
27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/652
		CVE ID : CVE-2021-0423		
27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/653
27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/654
	27-Sep-21	27-Sep-21 2.1 27-Sep-21 2.1	exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422  In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05385714.  CVE ID: CVE-2021-0423  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424  In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID : CVE-2021-0422  In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID : CVE-2021-0423  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05393787.  CVE ID : CVE-2021-0424  In memory management driver, there is a possible side channel information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: https://corp.mediatek.com/product-security-bulletin/Sept ember-2021  27-Sep-21  2.1  In memory management driver, there is a possible side channel information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: https://corp.mediatek.com/product-security-bulletin/Sept ember-2021  ALPS05403499; Issue ID: https://corp.mediatek.com/product-security-bulletin/Sept ember-2021

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID : CVE-2021-0425						
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/655				
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/656				
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/657				
mt6750	mt6750								
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp. mediatek.co	H-MED- MT67-				

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	m/product- security- bulletin/Sept ember-2021	061021/658
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/659
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/660
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp. mediatek.co m/product- security- bulletin/Sept	H-MED- MT67- 061021/661

CVSS Scoring Scale

0-1

5-6

6-7

7-8

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/662
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/663
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/664

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834.		
			CVE ID : CVE-2021-0612		
mt6750s					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/665
			CVE ID : CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/666
			CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/667

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/668
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/669
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/670
				https://ssam	H-MED-
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp. mediatek.co m/product-	MT67- 061021/671
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	security- bulletin/Sept ember-2021	
mt6752			CVE ID . CVE-2021-0012		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/672
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/673
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution  2-3 3-4 4-5 5-6	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/674

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/675
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/676
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/677

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810.		
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/678
			CVE ID : CVE-2021-0612		
mt6753			Υ .		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/679
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/680

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/681
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/682
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/683
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp. mediatek.co m/product-	H-MED- MT67- 061021/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privileg with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	e security- bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privileg with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	e https://corp. mediatek.co m/product-	H-MED- MT67- 061021/685
			CVE ID : CVE-2021-0612		
mt6755					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missin bounds check. This could leat to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	d https://corp.	H-MED- MT67- 061021/686
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	security- bulletin/Sept ember-2021	H-MED- MT67- 061021/687
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/688
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/689
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/690

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456.		
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/691
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/692
mt6755s					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/693
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	mediatek.co m/product- security- bulletin/Sept ember-2021	MT67- 061021/694
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/695
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/696
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp. mediatek.co m/product- security-	H-MED- MT67- 061021/697
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 255 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/698
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/699
mt6757					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/700
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

		exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.		
		CVE ID : CVE-2021-0422		
27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/701
		CVE ID: CVE-2021-0423		
27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/702
27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/703
	27-Sep-21	27-Sep-21 2.1 27-Sep-21 2.1	27-Sep-21  2.1  2.1  In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424  In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS0540059.	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2021-0425					
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/704			
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/705			
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/706			
mt6757c								
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp. mediatek.co	H-MED- MT67-			

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	m/product- security- bulletin/Sept ember-2021	061021/707
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/708
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/709
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp. mediatek.co m/product- security- bulletin/Sept	H-MED- MT67- 061021/710

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/711
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/712
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/713

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834.		
			CVE ID : CVE-2021-0612		
mt6757cd					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/714
			CVE ID : CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/715
			CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/716

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/717
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/718
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/719
				https://ssam	H-MED-
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp. mediatek.co m/product-	MT67- 061021/720
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	security- bulletin/Sept ember-2021	
mt6757ch					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/721
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/722
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution  2-3 3-4 4-5 5-6	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/723

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/724
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/725
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/726

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810.		
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/727
mt6750			CVE ID : CVE-2021-0612		
mt6758					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/728
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/729

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/730
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/731
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/732
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp. mediatek.co m/product-	H-MED- MT67- 061021/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	security- bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/734
			CVE ID : CVE-2021-0612		
mt6761					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/735
			CVE ID : CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/736

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/737
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/738
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/739

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456.		
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/740
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/741
mt6762					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/742
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	mediatek.co m/product- security- bulletin/Sept ember-2021	MT67- 061021/743
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/744
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/745
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp. mediatek.co m/product- security-	H-MED- MT67- 061021/746
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 Page 270 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/747
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/748
mt6763					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/749
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

o-21	2.1	exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422  In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional	https://corp.	
o-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information	https://corp.	
o-21	2.1	driver, there is a possible information disclosure due to uninitialized data. This could lead to local information	https://corp.	
		execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/750
		CVE ID : CVE-2021-0423		
o-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/751
o-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/752
			no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424  In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424  In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:  In memory management driver, there is a possible side channel information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/753
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/754
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/755
mt6765					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp. mediatek.co	H-MED- MT67-

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	m/product- security- bulletin/Sept ember-2021	061021/756
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/757
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/758
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp. mediatek.co m/product- security- bulletin/Sept	H-MED- MT67- 061021/759

6-7

7-8

8-9

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	ember-2021	
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/760
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/761
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/762

**2-3 3-4 4-5** 

1-2

0-1

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834.		
			CVE ID : CVE-2021-0612		
mt6768					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/763
			CVE ID : CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/764
			CVE ID : CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/765

6-7

**2-3 3-4 4-5** 

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/766
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/767
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/768
			In m4u, there is a possible	https://corp.	H-MED-
Use After Free	27-Sep-21	4.6	memory corruption due to a use after free. This could lead	MT67- 061021/769	
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	security- bulletin/Sept ember-2021	
mt6769			CVE ID . CVE-2021-0012		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/770
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05385714.  CVE ID: CVE-2021-0423		H-MED- MT67- 061021/771
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution  2-3 3-4 4-5 5-6	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/772

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/773
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/774
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/775

**2-3 3-4 4-5** 

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	& CVE ID Patch		
			ALPS05425810.			
			CVE ID: CVE-2021-0611			
Use After Free	er 27-Sep-21		In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/776	
			CVE ID : CVE-2021-0612			
mt6771			Υ .			
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/777	
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/778	

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution	https://corp. mediatek.co	
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787. CVE ID: CVE-2021-0424	m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/779
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/780
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/781
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp. mediatek.co m/product-	H-MED- MT67- 061021/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	security- bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/783
16880			CVE ID : CVE-2021-0612		
mt6779					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/784
			CVE ID : CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/785

Weakness	Publish Date	cvss	Description & CVE ID	NCIIPC ID	
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/786
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/787
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/788

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	NCIIPC ID	
			ALPS05411456.		
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	h m4u, there is a possible nemory corruption due to a se after free. This could lead to local escalation of privilege with System execution rivileges needed. User needed for exploitation. Patch ID: LPS05403499; Issue ID: LPS05425810.  VE ID: CVE-2021-0611		H-MED- MT67- 061021/789
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/790
Out-of- bounds Read	27-Sep-21	4	In ccu, there is a possible out of bounds read due to incorrect error handling. This could lead to information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827145; Issue ID: ALPS05827145.  CVE ID: CVE-2021-0660	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/791
mt6785					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp. mediatek.co	H-MED- MT67-
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 284 of 861	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			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	m/product- security- bulletin/Sept ember-2021	061021/792
Missing Initialization of Resource	27-Sep-21	2.1	n memory management driver, there is a possible information disclosure due to ininitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch D: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423		H-MED- MT67- 061021/793
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/794
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp. mediatek.co m/product- security- bulletin/Sept	H-MED- MT67- 061021/795

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059. CVE ID: CVE-2021-0425	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/796
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/797
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/798
CVSS Scoring Sca	ile <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 286 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			ALPS05425834.			
			CVE ID : CVE-2021-0612			
mt6795						
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/799	
			CVE ID : CVE-2021-0422			
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/800	
			CVE ID : CVE-2021-0423			
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/801	

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

CVSS Scoring Scale

Weakness	Publish Date	cvss	Des	criptio	n & CVE	ID	Pa	tch	NCI	IPC ID
			CVE ID:	CVE-2	2021-04	<b>424</b>				
N/A	27-Sep-21	2.1	driver, the channel is disclosure local information with no apprivilege interaction exploitatt ALPS054	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425					H-MEI MT67- 06102	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memodriver, the memory integer of lead to loo privilege execution User integer of ID: ALPSO 54	a possi ption du ow. This calation no addi ileges n on is not oloitatio 3499; Is 6.	ble ue to an could n of tional eeded. n. Patch sue ID:	mediat m/pro securit	duct- y- n/Sept	H-MEI MT67- 06102		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611				mediat m/pro securit	duct- cy- n/Sept	H-MEI MT67- 06102	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a						H-MEI MT67- 06102	
CVSS Scoring Sca	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	security- bulletin/Sept ember-2021	
mt6797			0011111 1 0011 1 0011		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/806
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/807
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/808

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/809
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/810
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/811

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810.		
			CVE ID : CVE-2021-0611		
Use After Free	27-Sen-21		In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/812
			CVE ID : CVE-2021-0612		
mt6799					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/813
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/814

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424		H-MED- MT67- 061021/815
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. closure ecution er ded for billead to https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/817
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead	https://corp. mediatek.co m/product-	H-MED- MT67- 061021/818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	security- bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT67- 061021/819
16000			CVE ID : CVE-2021-0612		
mt6833					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/820
			CVE ID: CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/821

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/822
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/823
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/824

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05411456.		
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  mediatek.c m/product security- bulletin/Se		https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/825
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/826
mt6853					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422		H-MED- MT68- 061021/827
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-
CVSS Scoring Sca	le 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	mediatek.co m/product- security- bulletin/Sept ember-2021	MT68- 061021/828
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/829
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/830
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp. mediatek.co m/product- security-	H-MED- MT68- 061021/831
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 296 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/832
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/833
			CVE ID : CVE-2021-0612		
Out-of- bounds Read	27-Sep-21	4	In ccu, there is a possible out of bounds read due to incorrect error handling. This could lead to information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827145; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/834

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05827145.		
			CVE ID : CVE-2021-0660		
mt6853t					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/835
			CVE ID : CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/836
			CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/837

Weakness	Publish Date	CVSS	Description	& CVE ID	Pat	tch	NCII	PC ID
			CVE ID : CVE-20	021-0424				
N/A	27-Sep-21	2.1	In memory mandriver, there is a channel information disclosure. This local information with no addition privileges needs interaction is not exploitation. Para ALPS05403499 ALPS05400059	a possible side ation could lead to on disclosure nal execution ed. User ot needed for tch ID: ; Issue ID:	https:/ mediat m/pro securit bulletin ember-	cek.co duct- cy- n/Sept	H-MEI MT68- 06102	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory mandriver, there is a memory corrupt integer overflow lead to local escaprivilege with mexecution privilege with mexecution privilege interaction needed for explain the explain	a possible ation due to an av. This could calation of a additional eges needed. In is not oitation. Patch 499; Issue ID:	https:/ mediat m/pro securit bulletin ember-	duct- y- n/Sept	H-MEI MT68- 06102	
Use After Free	27-Sep-21	4.6	In m4u, there is memory corrup use after free. T to local escalation with System exemprivileges needs interaction is not exploitation. Par ALPS05403499 ALPS05425810 CVE ID: CVE-20	https:/ mediat m/pro securit bulletii ember-	cek.co duct- cy- n/Sept	H-MEI MT68- 06102		
Use After Free	27-Sep-21	4.6	In m4u, there is memory corrup use after free. T	https:/ mediat m/pro	ek.co	H-MEI MT68- 06102		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	security- bulletin/Sept ember-2021	
mt6873					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/842
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05385714.  CVE ID: CVE-2021-0423	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/843
Improper Restriction of Operations within the Bounds of a	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution  2-3 3-4 4-5 5-6	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/844

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/845
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/846
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/847

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425810.		
			CVE ID: CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/848
Out-of- bounds Read	27-Sep-21	4	In ccu, there is a possible out of bounds read due to incorrect error handling. This could lead to information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05827145; Issue ID: ALPS05827145.  CVE ID: CVE-2021-0660	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/849
mt6875					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/850
Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	mediatek.co m/product- security- bulletin/Sept ember-2021	MT68- 061021/851
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/852
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/853
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp. mediatek.co m/product- security-	H-MED- MT68- 061021/854
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 Page 303 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Pato ID: ALPS05403499; Issue ID ALPS05411456.	ch	
			CVE ID : CVE-2021-0610		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privileg with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	https://corp. mediatek.co m/product-	H-MED- MT68- 061021/855
			CVE ID : CVE-2021-0611		
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privileg with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product-	H-MED- MT68- 061021/856
mt6877					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/857
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

				NCIIPC ID
		exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.		
		CVE ID : CVE-2021-0422		
27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/858
		CVE ID: CVE-2021-0423		
27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/859
27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/860
	27-Sep-21	27-Sep-21 2.1	27-Sep-21  2.1  ALPS05381071.  CVE ID: CVE-2021-0422  In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424  In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	27-Sep-21  2.1  2.1  2.1  2.1  2.1  2.1  2.1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0425		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/861
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/862
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/863
mt6883					
Improper Restriction	27-Sep-21	2.1	In memory management driver, there is a possible	https://corp. mediatek.co	H-MED- MT68-

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422	m/product- security- bulletin/Sept ember-2021	061021/864
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05385714.  CVE ID: CVE-2021-0423		H-MED- MT68- 061021/865
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/866
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure	https://corp. mediatek.co m/product- security- bulletin/Sept	H-MED- MT68- 061021/867

CVSS Scoring Scale

0-1

5-6

6-7

8-9

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	ember-2021	
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/868
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/869
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/870
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 308 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ALPS05425834.		
			CVE ID : CVE-2021-0612		
mt6885					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/871
			CVE ID : CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/872
			CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS05403499; Issue ID:  ALPS05393787.		H-MED- MT68- 061021/873

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	CVSS	De	escriptio	n & CVE	ID	Pa	tch	NCI	IPC ID
			CVE ID	: CVE-2	2021-0	124				
N/A	27-Sep-21	2.1	driver, channed disclosure local interaction with no privilege interaction exploits ALPS05	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425					H-MEI MT68- 06102	_
Integer Overflow or Wraparound	27-Sep-21	4.6	driver, memory integer lead to privileg execution User integed ID: ALP ALPS05	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.				//corp. tek.co duct- cy- n/Sept -2021	H-MEI MT68- 06102	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611				https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021		H-MEI MT68- 06102	
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead			https:/ mediat		H-MEI MT68- 06102		
CVSS Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privileges needed. User interaction is not needed exploitation. Patch ID: ALPS05403499; Issue ID ALPS05425834.	bulletin/Sept ember-2021 d for	
			CVE ID : CVE-2021-061	.2	
Out-of- bounds Read	27-Sep-21	4	In ccu, there is a possible of bounds read due to incorrect error handling could lead to informatio disclosure with System execution privileges need User interaction is not needed for exploitation. ID: ALPS05827145; Issu ALPS05827145.	H-MED- MT68- 061021/878	
			CVE ID : CVE-2021-066	50	
mt6889					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possibl system crash due to a m bounds check. This could to local denial of service no additional execution privileges needed. User interaction is not needed exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-042	e issing d lead https://corp. mediatek.co m/product-security-bulletin/Sept ember-2021	H-MED- MT68- 061021/879
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure of uninitialized data. This of lead to local information disclosure with no addit execution privileges nee	e mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/880
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/881
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/882
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/883

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

CVSS Scoring Scale

Use After Free  27-Sep-21  Use After Free  27-Sep-21  Use After Free  27-Sep-21  Use After Free  27-Sep-21  In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499;	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free  Use After Free  27-Sep-21  4.6  Use After Free  27-Sep-21  4.6  Use After Free  In memory management driver, there is a possible will be a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; I				ALPS05411456.		
Use After Free  27-Sep-21  4.6  Use After Free  27-Sep-21  4.6  Use After Free  4.6  Use After In matu, there is a possible memory corruption due to a use after free. This could lead to local descalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO5403499; Issue ID: A				CVE ID : CVE-2021-0610		
Use After Free 27-Sep-21 4.6		27-Sep-21	4.6	memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	mediatek.co m/product- security- bulletin/Sept	MT68-
Improper Restriction of Operations within the Bounds of a Memory Buffer  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05381071.  CVE ID: CVE-2021-0422  In memory management driver, there is a possible system crash due to a missing https://corp. mediatek.co m/product-security- bulletin/Sept ember-2021		27-Sep-21	4.6	memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.	mediatek.co m/product- security- bulletin/Sept	MT68-
Improper Restriction of Operations within the Bounds of a Memory Buffer  Odiver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05381071.  CVE ID: CVE-2021-0422   driver, there is a possible system crash due to a missing https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021  H-MED- MT68- 061021/886	mt6891					
Missing 27-Sep-21 2.1 In memory management https://corp. H-MED-	Restriction of Operations within the Bounds of a Memory	27-Sep-21	2.1	driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	mediatek.co m/product- security- bulletin/Sept	MT68-
	Missing	27-Sep-21	2.1	In memory management	https://corp.	H-MED-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID						
Initialization of Resource			driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423	mediatek.co m/product- security- bulletin/Sept ember-2021	MT68- 061021/887						
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/888						
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.  CVE ID: CVE-2021-0425	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/889						
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could	https://corp. mediatek.co m/product- security-	H-MED- MT68- 061021/890						
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 314 of 861	6-7 7-8	CVSS Scoring Scale						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	bulletin/Sept ember-2021					
			CVE ID : CVE-2021-0610						
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/891				
			CVE ID : CVE-2021-0611						
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/892				
mt6893									
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/893				
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

		·		NCIIPC ID
		exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.		
		CVE ID : CVE-2021-0422		
27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/894
		CVE ID : CVE-2021-0423		
27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/895
27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05400059.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/896
	27-Sep-21	27-Sep-21 2.1	27-Sep-21  2.1  ALPS05403499; Issue ID: ALPS05381071.  CVE ID : CVE-2021-0422  In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID : CVE-2021-0423  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID : CVE-2021-0424  In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID:	ALPS05403499; Issue ID: ALPS05381071.  CVE ID: CVE-2021-0422  In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.  CVE ID: CVE-2021-0423  In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.  CVE ID: CVE-2021-0424  In memory management driver, there is a possible side channel information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: https://corp. mediatek.co m/product-security-bulletin/Sept ember-2021  ALPS05403499; Issue ID: https://corp. mediatek.co m/product-security-bulletin/Sept ember-2021  ALPS05403499; Issue ID: https://corp. mediatek.co m/product-security-bulletin/Sept ember-2021  ALPS05403499; Issue ID: https://corp. mediatek.co m/product-security-bulletin/Sept ember-2021

				NCIIPC ID			
		CVE ID : CVE-2021-0425					
27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/897			
27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425810.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/898			
		CVE ID : CVE-2021-0611					
27-Sep-21	4.6	In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	H-MED- MT68- 061021/899			
Netgear							
gc108p							
16-Sep-21	8.3	Certain NETGEAR smart	https://kb.n	H-NET-GC10-			
	27-Sep-21 27-Sep-21	27-Sep-21 4.6  27-Sep-21 4.6	In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610  In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611  In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612	27-Sep-21  4.6  In memory management driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05411456.  CVE ID: CVE-2021-0610  In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05425810.  CVE ID: CVE-2021-0611  In m4u, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-0612  ALPS05425834.  CVE ID: CVE-2021-0612			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Authenticati			switches are affected by a \n	etgear.com/0	061021/900	
on			injection in the web UI's	00063978/S		
			password field, which - due to	ecurity-		
			several faulty aspects of the	Advisory-for-		
			authentication scheme -	Multiple-		
			allows the attacker to create	Vulnerabiliti		
			(or overwrite) a file with	es-on-Some-		
			specific content (e.g., the "2"	Smart-		
			string). This leads to admin	Switches-		
			session crafting and therefore	PSV-2021-		
			gaining full web UI admin	0140-PSV-		
			privileges by an	2021-0144-		
			unauthenticated attacker.	PSV-2021-		
			This affects GC108P before	0145		
			1.0.8.2, GC108PP before			
			1.0.8.2, GS108Tv3 before			
			7.0.7.2, GS110TPP before			
			7.0.7.2, GS110TPv3 before			
			7.0.7.2, GS110TUP before			
			1.0.5.3, GS308T before			
			1.0.3.2, GS310TP before			
			1.0.3.2, GS710TUP before			
			1.0.5.3, GS716TP before			
			1.0.4.2, GS716TPP before			
			1.0.4.2, GS724TPP before			
			2.0.6.3, GS724TPv2 before			
			2.0.6.3, GS728TPPv2 before			
			6.0.8.2, GS728TPv2 before			
			6.0.8.2, GS750E before			
			1.0.1.10, GS752TPP before			
			6.0.8.2, GS752TPv2 before			
			6.0.8.2, MS510TXM before			
			1.0.4.2, and MS510TXUP			
			before 1.0.4.2.			
			CVE ID : CVE-2021-41314			
gc108pp						
T			Certain NETGEAR smart	https://kb.n		
Improper	16.0 24	0.0	switches are affected by a \n	etgear.com/0	H-NET-GC10-	
Authenticati	16-Sep-21	8.3	injection in the web UI's	00063978/S	061021/901	
on			password field, which - due to	ecurity-	,	
CVSS Scoring Scale						

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
			several faulty aspects of the	Advisory-for-			
			authentication scheme -	Multiple-			
			allows the attacker to create	Vulnerabiliti			
			(or overwrite) a file with	es-on-Some-			
			specific content (e.g., the "2"	Smart-			
			string). This leads to admin	Switches-			
			session crafting and therefore	PSV-2021-			
			gaining full web UI admin	0140-PSV-			
			privileges by an	2021-0144-			
			unauthenticated attacker.	PSV-2021-			
			This affects GC108P before	0145			
			1.0.8.2, GC108PP before				
			1.0.8.2, GS108Tv3 before				
			7.0.7.2, GS110TPP before				
			7.0.7.2, GS110TPv3 before				
			7.0.7.2, GS110TUP before				
			1.0.5.3, GS308T before				
			1.0.3.2, GS310TP before				
			1.0.3.2, GS710TUP before				
			1.0.5.3, GS716TP before				
			1.0.4.2, GS716TPP before				
			1.0.4.2, GS724TPP before				
			2.0.6.3, GS724TPv2 before				
			2.0.6.3, GS728TPPv2 before				
			6.0.8.2, GS728TPv2 before				
			6.0.8.2, GS750E before				
			1.0.1.10, GS752TPP before				
			6.0.8.2, GS752TPv2 before				
			6.0.8.2, MS510TXM before				
			1.0.4.2, and MS510TXUP				
			before 1.0.4.2.				
			CVE ID : CVE-2021-41314				
gs108t							
8			Contain NETCEAR	latter c. 1/1/1			
			Certain NETGEAR smart	https://kb.n			
Improper			switches are affected by a \n	etgear.com/0			
Improper Authenticati	16-Sep-21	8.3	injection in the web UI's	00063978/S	H-NET-GS10-		
	10-3cp-21	0.5	password field, which - due to	ecurity-	061021/902		
on			several faulty aspects of the	Advisory-for-			
			authentication scheme -	Multiple-			
			allows the attacker to create	Vulnerabiliti			
CVSS Scoring Sca	CVSS Scoring Scale						
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10							

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			(or overwrite) a file with	es-on-Some-		
			specific content (e.g., the "2"	Smart-		
			string). This leads to admin	Switches-		
			session crafting and therefore	PSV-2021-		
			gaining full web UI admin	0140-PSV-		
			privileges by an	2021-0144-		
			unauthenticated attacker.	PSV-2021-		
			This affects GC108P before	0145		
			1.0.8.2, GC108PP before			
			1.0.8.2, GS108Tv3 before			
			7.0.7.2, GS110TPP before			
			7.0.7.2, GS110TPv3 before			
			7.0.7.2, GS110TUP before			
			1.0.5.3, GS308T before			
			1.0.3.2, GS310TP before			
			1.0.3.2, GS710TUP before			
			1.0.5.3, GS716TP before			
			1.0.4.2, GS716TPP before			
			1.0.4.2, GS724TPP before			
			2.0.6.3, GS724TPv2 before			
			2.0.6.3, GS728TPPv2 before			
			6.0.8.2, GS728TPv2 before			
			6.0.8.2, GS750E before			
			1.0.1.10, GS752TPP before			
			6.0.8.2, GS752TPv2 before			
			6.0.8.2, MS510TXM before			
			1.0.4.2, and MS510TXUP			
			before 1.0.4.2.			
			CVE ID: CVE-2021-41314			
gs110tp						
			Certain NETGEAR smart	https://kb.n		
			switches are affected by a \n	etgear.com/0		
			injection in the web UI's	00063978/S		
Improper			password field, which - due to	ecurity-		
Authenticati	16-Sep-21	8.3	several faulty aspects of the	Advisory-for-	H-NET-GS11-	
on	10 5cp 21	0.0	authentication scheme -	Multiple-	061021/903	
			allows the attacker to create	Vulnerabiliti		
			(or overwrite) a file with	es-on-Some-		
			specific content (e.g., the "2"	Smart-		
			string). This leads to admin	Switches-		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.3.2, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145		
gs110tpp						
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144-	H-NET-GS11- 061021/904	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.4.2, GS716TP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314	PSV-2021- 0145	
gs110tup					
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	H-NET-GS11- 061021/905
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.5.3, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314		
gs308t			CVE ID . CVE-2021-41514		
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	H-NET-GS30- 061021/906

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

16-Sep-21   Improper   Authenticati on   16-Sep-21   Improper   Authenticati on   16-Sep-21   Improper   Authenticati on   16-Sep-21   Improper   1.0.8.2, GS10TPP before   1.0.8.2, GS7.88TP before   1.0.4.2   GS7.88TP before   1.0.8.2   GS7.88TP before	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authenticati on  16-Sep-21  8.3  Certain NETGEAR smart switches are affected by a \n injection in the web Ul's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before  Total NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" Multiple-Vulnerabiliti es-on-Some-Smart-Switches-PSV-2021-0140-PSV-2021-0144-PSV-2021-0144-PSV-2021-0144-PSV-2021-0145				1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, GS752TPv2 before 1.0.4.2, and MS510TXUP		
Improper Authenticati on  16-Sep-21 on  16-Sep-21 on  Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before  7.0.7.2, GS110TUP before 1.0.5.3, GS308T before				CVE ID : CVE-2021-41314		
switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108TV3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before	gs310tp					
CVSS Scoring Scale	Authenticati			switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before	etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	061021/907

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314		
gs710tup					
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.5.3, GS716TPP before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	H-NET-GS71- 061021/908

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314		
gs716tp					
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS310TP before 1.0.3.2, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPPv2 before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	H-NET-GS71- 061021/909

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
gs716tpp			6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314		
Improper Authenticati on	16-Sep-21	8.3	switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS310TPV3 before 1.0.5.3, GS310TPV3 before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144-	H-NET-GS71- 061021/910
		1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before	PSV-2021- 0145		

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
gs724tp			6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID : CVE-2021-41314		
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 6.0.8.2, GS728TPV2 before 6.0.8.2, GS752TPP before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	H-NET-GS72- 061021/911

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.4.2.		
			CVE ID : CVE-2021-41314		
gs724tpp					
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before 1.0.3.2, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 6.0.8.2, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS7510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	H-NET-GS72- 061021/912

		CVSS	Description & CVE ID	Patch	NCIIPC ID
gs728tp					
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.3.2, GS716TP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	H-NET-GS72- 061021/913
gs728tpp					
Improper Authenticati	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n	https://kb.n etgear.com/0	H-NET-GS72-

			Description & CVE ID	Patch	NCIIPC ID
on			injection in the web UI's	00063978/S	061021/914
			password field, which - due to	ecurity-	
			several faulty aspects of the	Advisory-for-	
			authentication scheme -	Multiple-	
			allows the attacker to create	Vulnerabiliti	
			(or overwrite) a file with	es-on-Some-	
			specific content (e.g., the "2"	Smart-	
			string). This leads to admin	Switches-	
			session crafting and therefore	PSV-2021-	
			gaining full web UI admin	0140-PSV-	
			privileges by an	2021-0144-	
			unauthenticated attacker.	PSV-2021-	
			This affects GC108P before	0145	
			1.0.8.2, GC108PP before		
			1.0.8.2, GS108Tv3 before		
			7.0.7.2, GS110TPP before		
			7.0.7.2, GS110TPv3 before		
			7.0.7.2, GS110TUP before		
			1.0.5.3, GS308T before		
			1.0.3.2, GS310TP before		
			1.0.3.2, GS710TUP before		
			1.0.5.3, GS716TP before		
			1.0.4.2, GS716TPP before		
			1.0.4.2, GS724TPP before		
			2.0.6.3, GS724TPv2 before		
			2.0.6.3, GS728TPPv2 before		
			6.0.8.2, GS728TPv2 before		
			6.0.8.2, GS750E before		
			1.0.1.10, GS752TPP before		
			6.0.8.2, GS752TPv2 before		
			6.0.8.2, MS510TXM before		
			1.0.4.2, and MS510TXUP		
			before 1.0.4.2.		
			CVE ID : CVE-2021-41314		
gs750e					
03.000			Contain NETCEAD and and	https://l-l	
Improper			Certain NETGEAR smart	https://kb.n	
Authenticati	16-Sep-21	8.3	switches are affected by a \n	etgear.com/0	H-NET-GS75-
	10-3ep-21	0.5	injection in the web UI's	00063978/S	061021/915
on			password field, which - due to	ecurity-	
			several faulty aspects of the	Advisory-for-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication scheme -	Multiple-	
			allows the attacker to create	Vulnerabiliti	
			(or overwrite) a file with	es-on-Some-	
			specific content (e.g., the "2"	Smart-	
			string). This leads to admin	Switches-	
			session crafting and therefore	PSV-2021-	
			gaining full web UI admin	0140-PSV-	
			privileges by an	2021-0144-	
			unauthenticated attacker.	PSV-2021-	
			This affects GC108P before	0145	
			1.0.8.2, GC108PP before		
			1.0.8.2, GS108Tv3 before		
			7.0.7.2, GS110TPP before		
			7.0.7.2, GS110TPv3 before		
			7.0.7.2, GS110TUP before		
			1.0.5.3, GS308T before		
			1.0.3.2, GS310TP before		
			1.0.3.2, GS710TUP before		
			1.0.5.3, GS716TP before		
			1.0.4.2, GS716TPP before		
			1.0.4.2, GS724TPP before		
			2.0.6.3, GS724TPv2 before		
			2.0.6.3, GS728TPPv2 before		
			6.0.8.2, GS728TPv2 before		
			6.0.8.2, GS750E before		
			1.0.1.10, GS752TPP before		
			6.0.8.2, GS752TPv2 before		
			6.0.8.2, MS510TXM before		
			1.0.4.2, and MS510TXUP		
			before 1.0.4.2.		
			CVE ID: CVE-2021-41314		
gs752tp					
			Certain NETGEAR smart	https://kb.n	
			switches are affected by a \n	etgear.com/0	
Improper			injection in the web UI's	00063978/S	
Authenticati	16-Sep-21	8.3	password field, which - due to	ecurity-	H-NET-GS75-
	10-36h-71	0.5	several faulty aspects of the	Advisory-for-	061021/916
on			authentication scheme -	Multiple-	
			allows the attacker to create	Vulnerabiliti	
			(or overwrite) a file with	es-on-Some-	
0.455.5					
CVSS Scoring Scale					

gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.3.2, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS724TPV2 before 6.0.8.2, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.  CVE ID: CVE-2021-41314  ms510txm  Certain NETGEAR smart switches are affected by a \ninjection in the web UI's password field, which - due to several faulty aspects of the authentication scheme -		
Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due t several faulty aspects of the	0140-PSV- 2021-0144- PSV-2021- 0145	
switches are affected by a \n injection in the web UI's password field, which - due t several faulty aspects of the		
Authenticati on  16-Sep-21 8.3  8.3  allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefor gaining full web UI admin privileges by an unauthenticated attacker.	Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches-	H-NET-MS51- 061021/918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, GS750TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314		
r6020					
Improper Neutralizatio n of Special Elements used in a Command ('Command Injection')	17-Sep-21	9	setup.cgi on NETGEAR R6020 1.0.0.48 devices allows an admin to execute arbitrary shell commands via shell metacharacters in the ntp_server field.  CVE ID: CVE-2021-41383	N/A	H-NET-R602- 061021/920
Phoenixconta	ict				
axc_f_1152					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID: CVE-2021-34570	https://cert. vde.com/en/ advisories/V DE-2021- 029/	H-PHO-AXC 061021/921
axc_f_2152	•				

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID: CVE-2021-34570	https://cert. vde.com/en/ advisories/V DE-2021- 029/	H-PHO-AXC 061021/922
axc_f_2152_st	arterkit				l
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID: CVE-2021-34570	https://cert. vde.com/en/ advisories/V DE-2021- 029/	H-PHO-AXC 061021/923
axc_f_3152					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID: CVE-2021-34570	https://cert. vde.com/en/ advisories/V DE-2021- 029/	H-PHO-AXC 061021/924
plcnext_techr	nology_starte	rkit			
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID: CVE-2021-34570	https://cert. vde.com/en/ advisories/V DE-2021- 029/	H-PHO-PLCN- 061021/925
rfc_4072s					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON	https://cert. vde.com/en/ advisories/V DE-2021- 029/	H-PHO-RFC 061021/926
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			requests.						
			CVE ID: CVE-2021-34570						
Qualcomm	Qualcomm								
apq8009									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-APQ8- 061021/927				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-APQ8- 061021/928				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-APQ8- 061021/929				
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	[	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Snapd Snapd Snapd	ragon W	lobile, oice & M Jearable	es				
a 00000			CVEII	): CVE-	2021-3	0261				
apq8009w			Maall as	.:	C		1			
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd	s due to tion who option fe ement is ragon C ragon C ragon C ragon I ragon Ir	ature toggled	in vity, r IOT, I IOT,	_	comm. ompan luct- cy/bull august	_	A-APQ8- 21/930
			CVE II	O: CVE-	2021-19	939				
Use After Free	17-Sep-21	7.2	kernel becaus pointe Compt Conne Indust Mobile Weara Wired Netwo	graphicse of sto er in Snaute, Snap ectivity, Strial IOT e, Snapd ables, Sn Infrastr	es driver ring an i pdragon Snapdra , Snapdr ragon apdrago	invalid gon ragon on	_	comm. ompan luct- cy/bull nugust	_	A-APQ8- 21/931
					2021-19					
Use After Free	17-Sep-21	10	to imp device frame Snapd Snapd Snapd Snapd	oroper variable address in Snaperagon Caragon Caragon Caragon Caragon Caragon Ir	e can oc alidation s in PD F dragon A ompute, onnectiv onsume ndustria oice & M	n of P2P Request Auto, vity, r IOT,	com/c	comm. ompan luct- cy/bull nugust	_	A-APQ8- 21/932
CVSS Scoring Sca	ile <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consume IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-APQ8- 061021/933
			CVE ID : CVE-2021-30261		
apq8017					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939		H-QUA-APQ8- 061021/934
Use After Free	17-Sep-21	10	A use after free can occur do to improper validation of P2 device address in PD Reque frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-APQ8- 061021/935
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-APQ8- 061021/936
apq8037					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8- 061021/937
apq8053					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature	https://ww w.qualcomm. com/compan y/product-	H-QUA-APQ8- 061021/938
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-APQ8- 061021/939
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8- 061021/940
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://ww w.qualcomm. com/compan y/product- security/bull	H-QUA-APQ8- 061021/941

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Hottps://www.qualcomm.com/company/product-security/bull etins/august-2021-bulletin	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Conpute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wet Infrastructure and Networking CVE ID : CVE-2021-1976  The proper Input Validation  Improper Input Validation  17-Sep-21  17-Sep-21  18  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon water in Com/compan y/product-security/bull etins/august -2021-bulletin Validation  17-Sep-21  17-Sep-21  17-Sep-21  17-Sep-21  17-Sep-21  17-Sep-21  18  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Voice & Music, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID : CVE 2021-30261  H-QUA-APQ8-061021/943  H-QUA-APQ8-061021/943				Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	-2021-	
Use After Free  17-Sep-21  10  10  Inproper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261  CVE ID: CVE-2021-30261  Lampor Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	apq8064au			CVE 10 . CVE 2021 30201		
Improper Input Validation Validation Validation  Improper Input Validation Validation  Validation  Improper Input Validation Validation  Validation  Improper Input Validation Validation  Improper Input Validation  Validation  Improper Input Validation  Validation  Input Validation	Use After Free	17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	
Improper Input Validation Validation  17-Sep-21  17-Sep	apq8084					
apq8096au	Improper Input Validation	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	1
	apq8096au					

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8- 061021/944
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-APQ8- 061021/945
aqt1000					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-AQT1- 061021/946
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

		CVE ID : CVE-2021-1939		
17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-AQT1- 061021/947
17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-AQT1- 061021/948
17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-AR60- 061021/949
	17-Sep-21	17-Sep-21 7.2	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Consumer IOT, Snapdragon Wearables  CVE ID: CVE-2021-30261  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IOT,	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID : CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Industrial IOT, Snapdragon Wearables CVE ID : CVE-2021-30261  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command grow HLOS in Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-30261  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon consumer lot, Snapdragon Industrial lot, Snapdragon I

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
ar7420					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-AR74- 061021/950
ar8031	I.				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-AR80- 061021/951
ar8035					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	H-QUA-AR80- 061021/952
CVSS Scoring Sco	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	security/bull etins/august -2021- bulletin	
0000			CVE ID : CVE-2021-1976		
ar9380					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-AR93- 061021/953
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-AR93- 061021/954
csr6030					

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-CSR6- 061021/955
csr8811					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-CSR8- 061021/956
csra6620					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-CSRA- 061021/957
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976		
csra6640			0.2.2.0.2.2.2.2.7.0		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-CSRA- 061021/958
csrb31024			CVE ID : CVE-2021-1976		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-CSRB- 061021/959
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://ww w.qualcomm. com/compan y/product-	H-QUA-CSRB- 061021/960

2-3 3-4 4-5

5-6

6-7

7-8

8-9

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	security/bull etins/august -2021- bulletin	
fsm10055					
Use After Free	17-Sep-21	10	A use after free can occur du to improper validation of P2 device address in PD Reques frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	P	H-QUA-FSM1- 061021/961
fsm10056					
Use After Free	17-Sep-21	10	A use after free can occur du to improper validation of P2 device address in PD Reques frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	Р	H-QUA-FSM1- 061021/962
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Des	scriptio	n & CVE	ID	Pa	tch	NCI	IPC ID
ipq4018										
Use After Free	17-Sep-21	10	A use aft to impro device ad frame in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra	oper vanddress Snapo gon Co gon Co gon In gon W gon W gon W icture king	alidation in PD R dragon A ompute, onnective onsumen dustrial oice & M Yearable Vired and	equest Auto, Pity, FIOT, IOT, Susic,	•	comm. compan luct- cy/bull nugust	_	A-IPQ4- 21/963
ipq4019			CVE ID.	CVL						
Use After Free	17-Sep-21	10	A use aft to impro device ad frame in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Composition	oper vanddress Snapo gon Co gon Co gon In gon W gon W gon W icture ting	alidation in PD R dragon A ompute, onnective onsumen dustrial oice & M Yearable Vired and	equest Auto, hity, FIOT, IOT, susic, s,	_	comm. ompan luct- y/bull nugust	_	A-IPQ4- 21/964
ipq4028							I			
Use After Free	17-Sep-21	10	A use aft to impro device ac frame in Snapdra Snapdra Snapdra Snapdra	oper va ddress Snapo gon Co gon Co gon Co	alidation s in PD R dragon A ompute, onnectiv	equest Auto, rity,	_	comm. ompan luct- cy/bull nugust	_	A-IPQ4- 21/965
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	bulletin	
ipq4029					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ4- 061021/966
ipq5010					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ5- 061021/967
ipq5018					
	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-IPQ5-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/968
ipq5028					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ5- 061021/969
ipq6000					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ6- 061021/970
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1976		
ipq6005					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ6- 061021/971
ipq6010					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ6- 061021/972
ipq6018					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://ww w.qualcomm. com/compan	H-QUA-IPQ6- 061021/973
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976	y/product- security/bull etins/august -2021- bulletin	
ipq6028					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ6- 061021/974
ipq8064					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ8- 061021/975
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ8- 061021/976
ipq8065					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8- 061021/977
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8- 061021/978

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1976		
ipq8068					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ8- 061021/979
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8- 061021/980
ipq8069					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ8- 061021/981
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ8- 061021/982
ipq8070			0.2.2.10.2.2021 1376		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ8- 061021/983
ipq8070a					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	H-QUA-IPQ8- 061021/984

**2-3 3-4 4-5** 

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976	security/bull etins/august -2021- bulletin	
ipq8071					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8- 061021/985
ipq8071a					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ8- 061021/986
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
ipq8072					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ8- 061021/987
ipq8072a					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8- 061021/988
ipq8074					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA-IPQ8- 061021/989
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	-2021- bulletin	
in a 0 0 7 4 a			CVE ID : CVE-2021-1976		
ipq8074a	T				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8- 061021/990
ipq8076					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8- 061021/991

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	De	scriptio	n & CVE	ID	Pa	tch	NCI	IPC ID
ipq8076a										
Use After Free	17-Sep-21	10	A use aft to impro device a frame in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Infrastra Network	oper vanddress Snapo Igon Co Igon Co Igon In Igon W Igon W Igon W Igon W Icture Iking	alidation in PD R dragon A compute, connective consumen dustrial coice & M Vearable Vired and	a of P2P dequest Auto, rity, r IOT, IOT, usic, s,	_	comm. compan luct- cy/bull nugust	_	A-IPQ8- 21/992
ipq8078			CVLID.							
Use After Free	17-Sep-21	10	A use aft to impro device a frame in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra CVE ID:	oper vanddress Snape Igon Co Igon Co Igon In Igon W	alidation is in PD R dragon A compute, connective consumen dustrial coice & M Yearable Vired and	a of P2P dequest Auto, rity, r IOT, IOT, usic, s,	_	comm. compan luct- y/bull nugust	_	A-IPQ8- 21/993
ipq8078a							1		1	
Use After Free	17-Sep-21	10	A use aft to impro device a frame in Snapdra Snapdra Snapdra Snapdra	oper va ddress Snapo Igon Co Igon Co	alidation s in PD R dragon A ompute, onnectiv	of P2P Request Auto, rity,	_	comm. ompan luct- cy/bull nugust	_	A-IPQ8- 21/994
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	bulletin	
ipq8173					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8- 061021/995
ipq8174					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-IPQ8- 061021/996
mdm8207					
	17-Sep-21	7.2	Possible integer and heap	https://ww	H-QUA-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	MDM8- 061021/997
mdm8215					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MDM8- 061021/998
mdm8215m					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MDM8- 061021/999
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Desc	cription & C	VE ID	Pa	tch	NCI	IPC ID
			CVE ID : (	CVE-2021	-30261				
mdm8615m									
Improper Input Validation	17-Sep-21	7.2	Possible in overflow command while han template from HLO Auto, Snap IOT, Snap IOT, Snap Snapdrag Snapdrag Snapdrag CVE ID: (	due to lact I size valid Idling bead update co S in Snapo pdragon Io dragon Io on Mobile on Voice & on Weara	k of input lation con mmand dragon consumer dustrial T, & Music, bles	com/c y/prod securi	comm. compan duct- ty/bull august	H-QUA MDM8 06102	
mdm9150									
Use After Free	17-Sep-21	10	to improp	oer validated dress in P. Snapdrago on Computon Consurton Industron Wearal on Wearal on Wired on Wired on Mired	ite, ctivity, mer IOT, rial IOT, & Music, bles,	https:/ w.qua com/c y/proc securi	dcomm. compan duct- ty/bull august	H-QUA MDM9 06102	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,  https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin		H-QUA MDM9 06102				
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
mdm9205					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MDM9- 061021/1003
mdm9206					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MDM9- 061021/1004
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://ww w.qualcomm. com/compan y/product- security/bull	H-QUA- MDM9- 061021/1005

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	etins/august -2021- bulletin	
mdm9207					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MDM9- 061021/1006
mdm9215					L
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MDM9- 061021/1007
mdm9230					
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	H-QUA-
CVSS Scoring Sc	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	MDM9- 061021/1008
mdm9250					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MDM9- 061021/1009
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MDM9- 061021/1010

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
mdm9310	L				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MDM9- 061021/1011
mdm9330					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MDM9- 061021/1012
mdm9607					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MDM9- 061021/1013
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MDM9- 061021/1014
mdm9615					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MDM9- 061021/1015
mdm9615m					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://ww w.qualcomm. com/compan y/product-	H-QUA- MDM9- 061021/1016

6-7

7-8

8-9

9-10

2-3 3-4 4-5

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august -2021- bulletin	
mdm9625			CVE ID : CVE-2021-30261		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MDM9- 061021/1017
mdm9626					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MDM9- 061021/1018

1-2

0-1

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Improper Input Validation  Improper Improper Input Validation  Improper Inp	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free 17-Sep-21 10 10	mdm9628					
Improper Input Validation  Validation  Improper Input Validation  Improper		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	=
Improper Input Validation Validation  To Sep-21  Improper Input Validation  Improper Input Validation  Validation  Validation  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,  Possible integer and heap overflow due to lack of input w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin	Input	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	_
Improper Input Validation  17-Sep-21  Total Parameters overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT,  Auto Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT,    https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin	mdm9630					
Silapul agoli Mobile,	Input	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music,		
			Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
mdm9635m					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MDM9- 061021/1022
mdm9640					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MDM9- 061021/1023
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA- MDM9- 061021/1024

6-7

7-8

8-9

9-10

2-3 3-4 4-5

1-2

0-1

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	-2021- bulletin	
mdm9645					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MDM9- 061021/1025
mdm9650					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MDM9- 061021/1026
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://ww w.qualcomm.	H-QUA- MDM9-

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	com/compan y/product- security/bull etins/august -2021- bulletin	061021/1027
mdm9655					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MDM9- 061021/1028
msm8108					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MSM8- 061021/1029
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descript	ion & CVE	ID	Pa	tch	NCI	IPC ID
msm8208									
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			com/c y/prod securit	comm. ompan duct- ty/bull august	H-QUA MSM8 06102	
msm8209									
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			com/c y/prod	comm. ompan duct- ty/bull august	H-QUA MSM8 06102	
msm8608									
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,			com/c y/prod securit	comm. ompan duct- ty/bull august	H-QUA MSM8 06102	
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			_	ragon V						
				ragon W						
			CVEII	D : CVE-	2021-30	)261				
msm8909w									ı	
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	ointer d s due to tion whe ption feement is ragon A ragon C ragon C ragon C ragon C ragon W	imprope en the ature toggled uto, ompute, onnectiv onsume idustria	in vity, r IOT, l IOT, s	com/c	comm. ompan duct- ty/bull august	H-QUA MSM8 06102	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			com/c	comm. ompan duct- ty/bull august	H-QUA MSM8 06102		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired			com/c	comm. ompan duct- ty/bull august	H-QUA MSM8 06102		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pa	tch	NCI	IPC ID	
			Infras Netwo	tructure orking	and						
				D : CVE-	2021-19	976					
Improper Input Validation	17-Sep-21	7.2	overfl comm while templ from I Auto, IOT, S IOT, S Snapd Snapd	ow due fand size handling ate upda HLOS in Snapdrag napdrag ragon Waragon Wara	to lack of validation to comment	f input ion nand igon sumer strial	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		H-QUA MSM8 06102		
			CVE II	D : CVE-	2021-3	0261					
msm8917	msm8917										
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939		-	comm. ompan luct- cy/bull august	H-QUA MSM8 06102			
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,		•	comm. ompan luct- cy/bull august	H-QUA MSM8 06102				
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976						
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MSM8- 061021/1039				
msm8920									
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MSM8- 061021/1040				
msm8937									
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA- MSM8- 061021/1041				
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 379 of 861	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	-2021- bulletin	
msm8940					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MSM8- 061021/1042
msm8953					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MSM8- 061021/1043
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon	https://ww w.qualcomm. com/compan y/product-	H-QUA- MSM8- 061021/1044

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947	security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MSM8- 061021/1045
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MSM8- 061021/1046
msm8976					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://ww w.qualcomm. com/compan	H-QUA- MSM8- 061021/1047
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	y/product- security/bull etins/august -2021- bulletin	
msm8976sg				<u>I</u>	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MSM8- 061021/1048
msm8996au					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- MSM8- 061021/1049
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- MSM8- 061021/1050
pmp8074					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-PMP8- 061021/1051
qca1990					
Improper Input Validation	command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consum		overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA1- 061021/1052
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 383 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
4004			CVE ID : CVE-2021-30201		
qca4004				I	l .
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA4- 061021/1053
qca4020					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA4- 061021/1054
qca4024				,	,
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-QCA4- 061021/1055
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Snapd Snapd Snapd Infrast Netwo	Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976			bulleti	n		
qca6174										
Use After Free	17-Sep-21	10	to imp device frame Snapd Snapd Snapd Snapd Snapd Snapd Infrast Netwo	after free proper value address in Snape ragon Co ragon Ir ragon W ragon W ragon W ragon W ragon W ragon W ragon W	alidations in PD Formal Ampute, compute, consumerative and waterable and	of P2P Request Auto, rity, r IOT, I IOT, Iusic, s,	_	comm. compan luct- cy/bull nugust	_	A-QCA6- 21/1056
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261		_	comm. compan luct- cy/bull nugust	_	A-QCA6- 21/1057		
qca6174a										
NULL Pointer	17-Sep-21	4.9	_	ointer de due to i			https:/ w.qual	/ww comm.	_	A-QCA6- 21/1058
CVSS Scoring Sca	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Dereference			validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	com/compan y/product- security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1059
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1060
qca6310					
	17-Sep-21	4.9	Null pointer dereference	https://ww	H-QUA-QCA6-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/1061
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1062
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1063
qca6320					
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sen-21   7.2		Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1064
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1065
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1066

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6335					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1067
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6- 061021/1068
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1069
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description & CVE ID				tch	NCI	IPC ID
			CVE II	) : CVE-2	2021-30	0261				
qca6390										
NULL Pointer Dereference	17-Sep-21	4.9	occurs validat preem enable Snapd Snapd Snapd Snapd Snapd	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939				//ww comm. ompan duct- ty/bull august	_	A-QCA6- 21/1070
			CVEIL	) : CVE-	2021-19	939				
Use After Free	17-Sep-21	7.2	kernel becaus pointe Compu Conne Indust Mobile Weara Wired Netwo	pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		1	A-QCA6- 21/1071	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			com/c y/prod securit	comm. ompan duct- ty/bull august	_	A-QCA6- 21/1072	
CVSS Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description & CVE ID				itch	NCI	PC ID
			CVE II	O : CVE-	2021-1	976				
Improper Input Validation	17-Sep-21	7.2	overflocomm while templa from I Auto, S IOT, Si Snapd Snapd Snapd	Possible integer and heap overflow due to lack of input command size validation while handling beacon remplate update command from HLOS in Snapdragon Auto, Snapdragon Consumer OT, Snapdragon Industrial OT, Snapdragon Mobile, Snapdragon Wearables CVE ID: CVE-2021-30261				//ww lcomm. compan duct- ty/bull august -	_	a-QCA6- 1/1073
qca6391										
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939		https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin		_	1-QCA6- 1/1074	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947			com/o y/pro securi	comm. compan duct- ty/bull august	_	1-QCA6- 1/1075	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1076
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6- 061021/1077
qca6420					
NULL Pointer Dereference	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1078	
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 392 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976 Possible integer and heap		https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6- 061021/1079	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1080
qca6421					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1081
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descript	Pa	tch	NCI	IPC ID		
			Snapdragon V	Wearable	S				
			CVE ID : CVE	-2021-1	939				
Improper Input Validation	17-Sep-21	7.2	Possible integoverflow due command size while handling template updefrom HLOS in Auto, Snapdra IOT, Snapdra IOT, Snapdra Snapdragon I S	com/c y/prod securit	comm. ompan duct- ty/bull august	_	A-QCA6- 1/1082		
qca6426									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables		https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin			A-QCA6- 1/1083	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		com/c y/prod securit	comm. ompan duct- ty/bull august	_	A-QCA6- 1/1084	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1947		
Use After Free	Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976  Possible integer and heap		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1085	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1086
qca6428					
Use After Free	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1087	
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Snapdragon Wired Infrastructure and Networking   CVE ID : CVE-2021-1976   CVE ID : CVE-2021-1939   C	Weakness	Publish Date	CVSS	Description 8	& CVE ID	Patch	1	NCI	IPC ID
NULL Pointer Dereference  17-Sep-21  Use After Free  17-Sep-21  Improper Imput Validation  Improper Imput Validation  Interport Validation  Interpore Imput Validation  Interpore Validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mustrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Consumer  17-Sep-21  10-Sep-21  1				Infrastructure an Networking	d				
NULL Pointer Dereference  17-Sep-21  Use After Free  17-Sep-21  Use After Free  17-Sep-21  Improper Input Validation  Improper Input Validation  Inproper Input Validation  Input Validation  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Consumer  Improper Input Validation  17-Sep-21  Validation  Null pointer dereference occur due to improper validation when the preemption feature enablement is toggled in Snapdragon Consumer  Improper lack the proper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Consumer  Improper lack the proper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Consumer  Improper lack the proper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Consumer  Improper lack the proper validation when the preemption feature enables and the product-security bull etins/august validation when the preemption feature enables and the product-security bull etins/august validation when the product-security bull etins/august validation wall the product validation wall the product validati	gca6430			CVE ID . CVE-20	21-19/0				
Use After Free  17-Sep-21  Improper Input Validation  Inspect Inspect Validation  Inspect Input	NULL Pointer	17-Sep-21	4.9	occurs due to important validation when to preemption feature enablement is tog Snapdragon Auto Snapdragon Company Snapdragon Consumption Snapdragon Indu Snapdragon Wear	proper the ggled in o, pute, nectivity, sumer IOT, estrial IOT, rables	w.qualco com/con y/productions security/ etins/aug- -2021-	omm. npan ct- /bull	_	•
Improper Input Validation  Validation  17-Sep-21  Validation  The proper Input Validation Validation Validation  Validation  The proper Input Validation Validation Validation Validation  The proper Input Validation Valid		17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		w.qualco com/con y/productions security/ etins/aug- -2021-	omm. npan ct- /bull	_	•
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Input	17-Sep-21	7.2	overflow due to l command size va while handling be template update from HLOS in Sna Auto, Snapdragon IOT, Snapdragon	w.qualco com/con y/productions security/ etins/aug- -2021-	omm. npan ct- /bull	_	•	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261		
qca6431					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1091
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1092
qca6436					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA-QCA6- 061021/1093

6-7

7-8

8-9

9-10

2-3 3-4 4-5

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	-2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1094
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1095
qca6438					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcomm. com/compan y/product- security/bull	H-QUA-QCA6- 061021/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976	etins/august -2021- bulletin	
qca6564					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2F device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		H-QUA-QCA6- 061021/1097
qca6564a					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2F device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		H-QUA-QCA6- 061021/1098
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261		H-QUA-QCA6- 061021/1099
qca6564au					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6- 061021/1100
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1101

1-2

0-1

5-6

6-7

8-9

9-10

7-8

Weakness	Publish Date	CVSS	С	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Snapd	ragon W	/earable	!S				
			CVE IE	) : CVE-	2021-3	0261				
qca6574										
NULL Pointer Dereference	17-Sep-21	4.9	occurs validat preem enable Snapdi Snapdi Snapdi Snapdi Snapdi	preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		_	A-QCA6- 21/1102	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,		•	comm. ompan luct- cy/bull august	_	A-QCA6- 21/1103		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,			com/c	comm. ompan luct- cy/bull august	_	A-QCA6- 21/1104	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
qca6574a			CVEID : CVE 2021 30201		
NULL			Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	H-QUA-QCA6-
Pointer Dereference	17-Sep-21	4.9	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	security/bull etins/august -2021- bulletin	061021/1105
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1106
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1107

Pointer Dereference  17-Sep-21  4.9  Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon  17-Sep-21  10  Snapdragon Compute, Snapdragon Auto, Snapdragon Compute, Sn	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference  17-Sep-21  Use After Free  17-Sep-21  Use After Free  17-Sep-21  Possible integer and heap overflow due to lack of input tomput Improper Input  17-Sep-21  Inproper Input  17-Sep-21  Integrated and respectively and a constant of the process of the of th				Snapdragon Voice & Music, Snapdragon Wearables		
NULL Pointer Dereference  17-Sep-21  Use After Free  17-Sep-21  18-Sep-21  18-Sep-21  19-Sep-21  19-Sep-21  19-Sep-21  19-Sep-21  19-Sep-21  10-Sep-21  10	qca6574au					
to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, w.qualcomm. com/compan w.qualcomm. com/compan y/product- H-QUA-Compan y/product- H-QUA-Co	Pointer	17-Sep-21	4.9	occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-QCA6- 061021/1108
overflow due to lack of input command size validation while handling beacon w.qualcomm.  The proper where the secondary overflow due to lack of input com/compan y/product-		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-QCA6- 061021/1109
Validation  template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial  security/bull etins/august -2021- bulletin	Input	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-QCA6- 061021/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261		
qca6584					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1111
qca6584au					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1112
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://ww w.qualcomm. com/compan y/product-	H-QUA-QCA6- 061021/1113

CVSS Scoring Scale

0-1

5-6

6-7

8-9

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	security/bull etins/august -2021- bulletin	
qca6595					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6- 061021/1114
qca6595au					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6- 061021/1115
Use After	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-QCA6-
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 405 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/1116
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6- 061021/1117
qca6694					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1118

1-2

0-1

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID: CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon emplate update command from HLOS in Snapdragon Consumer OT, Snapdragon Industrial OT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  EVE ID: CVE-2021-30261  https://www.qualcomm.com/company/product-security/bull etins/august-2021-bulletin		H-QUA-QCA6- 061021/1119
qca6694au					
Improper Input Validation	proper out 17-Sep-21 7.2 Auto IOT, Snap Snap Snap		Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6- 061021/1120
qca6696					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA6- 061021/1121
CVSS Scoring Sca	ile <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CV	E ID	Pate	ch	NCI	IPC ID
			Snapdragon Consumo Snapdragon Industria Snapdragon Wearabl	al IOT,				
			CVE ID : CVE-2021-1	939				
Use After Free	17-Sep-21	10	A use after free can o to improper validation device address in PD frame in Snapdragon Snapdragon Computer Snapdragon Connection Snapdragon Industrial Snapdragon Wearable Snapdragon Wearable Snapdragon Wired Infrastructure and Networking	n of P2P Request Auto, e, vity, er IOT, al IOT, Music,	https://w.qualcom/com/co y/produsecurity etins/au -2021- bulletin	omm. ompan uct- y/bull ugust	_	A-QCA6- 1/1122
			CVE ID : CVE-2021-1	976				
Improper Input Validation	17-Sep-21	7.2	template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,		https:// w.qualc com/co y/prode security etins/as -2021- bulletin	omm. ompan uct- y/bull ugust		A-QCA6- 1/1123
qca7500								
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,		https:// w.qualc com/co y/produ security etins/au -2021-	comm. mpan uct- 7/bull	_	A-QCA7- 1/1124
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	bulletin	
qca7520					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA7- 061021/1125
qca7550					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA7- 061021/1126
					l

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA8- 061021/1127
qca8075					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA8- 061021/1128
qca8081					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA8- 061021/1129
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID: CVE-2021-1976		
qca8337					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA8- 061021/1130
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA8- 061021/1131
qca9367					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcomm. com/compan y/product- security/bull	H-QUA-QCA9- 061021/1132
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Descripti	on & CVE	ID	Pat	ch.	NCI	IPC ID
			Snapdragon C Snapdragon I Snapdragon I Snapdragon I Snapdragon I Snapdragon I Infrastructure Networking	Consume ndustrial Voice & M Vearable Vired e and	r IOT, I IOT, Iusic, s,	etins/a -2021- bulletin			
Improper Input Validation	17-Sep-21	7.2	Possible integoverflow due command size while handling template upd from HLOS in Auto, Snapdrag IOT, Snapdrag IOT, Snapdrag Snapdragon Manapdragon Man	to lack of evalidating beaconstate comments of the second	f input ion nand igon sumer strial lusic, s	https:/ w.qual- com/co y/prod securit etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	_	A-QCA9- 1/1133
qca9377									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer of occurs due to validation who preemption for enablement is Snapdragon of CVE ID : CVE	improperien the eature stoggled Auto, Compute, Connective Consumer and wastrial Wearable	in vity, r IOT, I IOT, s	https:/ w.qual- com/co y/prod securit etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	•	A-QCA9- 1/1134
Use After Free	17-Sep-21	10	A use after free to improper v device address frame in Snap	validatior ss in PD F	of P2P Request	https:/ w.qual- com/co y/prod	comm.	_	A-QCA9- 1/1135
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976	security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1136
qca9379					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1137
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://ww w.qualcomm. com/compan	H-QUA-QCA9- 061021/1138
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	y/product- security/bull etins/august -2021- bulletin	
qca9531					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1139
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1140

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9- 061021/1141
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1142
qca9561					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9- 061021/1143
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1144
qca9563					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1145
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9- 061021/1146

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1976		
qca9880					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1147
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9- 061021/1148
qca9882					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1149
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur do to improper validation of P2 device address in PD Reque frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan	H-QUA-QCA9- 061021/1150
qca9886			CVE ID : CVE-2021-1970		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability kernel graphics driver because of storing an invalidation pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947		H-QUA-QCA9- 061021/1151
Use After Free	17-Sep-21	10	A use after free can occur do to improper validation of P2 device address in PD Reque frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA-QCA9- 061021/1152
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Free 17-Sep-21 7.2 Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wered Infrastructure and Networking CVE ID: CVE-2021-1976  Qca9888  Use After Free 17-Sep-21 7.2 Use-after-free vulnerability in kernel graphics driver because of storing an invalid H-QUA-QCA9 061021/1155	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free  17-Sep-21  Use After Free  17-Sep-21  17-Sep-21  Use After Free  Use After Free  17-Sep-21  Use After Free  17-Sep-21  Use After Free  17-Sep-21  Use After Free  Use After Free  17-Sep-21  Use After Free  Use After Free  Use After Free  I-QUA-QCA9  Use After Free  Use After Free  Use After Free  Use After Free  I-QUA-QCA9  Use After Free  Use After Free  Use After Free  I-QUA-QCA9  Use After Free  Use After Free  I-QUA-QCA9  Use After Free  Use After Free  Use After Free  I-QUA-QCA9  Of1021/115				Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
Sep	qca9887					
Use After Free  17-Sep-21  Use After Free  17-Sep-21  Use After Free  17-Sep-21  10  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1976  Qca9888  Use After Free  17-Sep-21  7.2  Use-after-free vulnerability in kernel graphics driver because of storing an invalid  H-QUA-QCA9 061021/1153		17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-QCA9- 061021/1153
Use After Free  17-Sep-21  Use After Free  17-Sep-21  10  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Qca9888  Use After Free  17-Sep-21  7.2  Use-after-free vulnerability in kernel graphics driver because of storing an invalid  To improper validation of P2P device address in PD Request https://ww w.qualcomm. because of storing an invalid  https://ww w.qualcomm. https://ww w.qualcomm. com/compan  H-QUA-QCA9  061021/1153				CVE ID : CVE-2021-1947		
Use After Free 17-Sep-21 7.2 Use-after-free vulnerability in kernel graphics driver because of storing an invalid com/compan 061021/1155		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-QCA9- 061021/1154
Use After Free 17-Sep-21 7.2 kernel graphics driver because of storing an invalid com/compan 061021/1155	qca9888					
pointer in snaparagon   y/product-		17-Sep-21	7.2	kernel graphics driver	w.qualcomm.	H-QUA-QCA9- 061021/1155

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	security/bull etins/august -2021- bulletin	
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9- 061021/1156
qca9889					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9- 061021/1157
Use After Free  CVSS Scoring Sca	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,  2-3 3-4 4-5 5-6	https://ww w.qualcomm. com/compan y/product-	H-QUA-QCA9- 061021/1158

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	security/bull etins/august -2021- bulletin	
qca9896			CVEID. CVE-2021-17/0		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1159
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1160
qca9898					

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1161
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1162
qca9980					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9- 061021/1163
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1164
qca9982					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9- 061021/1165
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9- 061021/1166

0-1

CVSS Scoring Scale

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1976		
qca9984					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9- 061021/1167
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9- 061021/1168
qca9985					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1169
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		
qca9986					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1170
qca9987					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1171
qca9988					
	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-QCA9-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/1172
qca9990					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1173
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCA9- 061021/1174

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pa	tch	NCI	IPC ID
			CVE ID	: CVE-2	2021-19	976				
qca9992										
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947				_	comm. ompan luct- cy/bull august	_	A-QCA9- 1/1175
			CVE ID	: CVE-2	2021-19	947				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976			•	comm. ompan duct- cy/bull august		A-QCA9- 1/1176	
qca9994										
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and			_	comm. ompan luct- cy/bull august	_	A-QCA9- 1/1177	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Netwo	rking						
			CVE II	O: CVE-	2021-19	947				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking				•	comm. ompan duct- cy/bull august	_	A-QCA9- :1/1178
			CVE II	O: CVE-	2021-19	976				
qcm2290										
Use After Free	17-Sep-21	7.2	kernel becaus pointe Compt Conne Indust Mobile Weara Wired Netwo	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			_	comm. ompan luct- cy/bull august	H-QUA QCM2 06102	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,			•	comm. ompan luct- cy/bull august	H-QUA QCM2 06102		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
qcm4290			CVE ID : CVE-2021-1976		
qciii4290			Use-after-free vulnerability i	n	
Use After Free	17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		H-QUA- QCM4- 061021/1181
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur du to improper validation of P2 device address in PD Reques frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	P	H-QUA- QCM4- 061021/1182
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial	com/compan y/product- security/bull etins/august	H-QUA- QCM4- 061021/1183
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261		
acm6125			CVE ID: CVE-2021-30201		
<b>qcm6125</b> Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- QCM6- 061021/1184
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2F device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	1	H-QUA- QCM6- 061021/1185
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA- QCM6- 061021/1186
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	bulletin	
qcn3018			CVE ID . CVE-2021-30201		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCN3- 061021/1187
qcn5021					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCN5- 061021/1188
qcn5022					
Use After	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-QCN5-

device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  Use After Free  17-Sep-21  Use After Free  17-Sep-21  Use After Free  17-Sep-21  Io  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID : CVE-2021-1976  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Wired Infrastructure and Networking  CVE ID : CVE-2021-1976  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, Snapdragon Auto, Snapdragon Compute,	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  T7-Sep-21  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Mired Infrastructure and Networking  CVE ID: CVE-2021-1976  T7-Sep-21  T8-Sep-21  T8-QUA-QCN5-Security/bull etins/august -2021-security/bull etins/august -2021-secu	Free			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	com/compan y/product- security/bull etins/august -2021-	061021/1189
Use After Free  17-Sep-21  10  10  10  10  10  10  10  10  10	qcn5024					
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Voice & Music,  A use after free can occur due to improper validation of P2P https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-QCN5- 061021/1190
Use After Free  17-Sep-21  10  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Voice & Music,  bulletin  https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021- bulletin	qcn5052					
		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-QCN5- 061021/1191

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1976		
qcn5054					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCN5- 061021/1192
qcn5064					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCN5- 061021/1193
qcn5121					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://ww w.qualcomm. com/compan	H-QUA-QCN5- 061021/1194
CVSS Scoring Sca	le 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			rame in Snapdragon Auto, Inapdragon Compute, Inapdragon Connectivity, Inapdragon Consumer IOT, Inapdragon Industrial IOT, Inapdragon Voice & Music, Inapdragon Wearables, Inapdragon Wired Infrastructure and Idetworking  EVE ID: CVE-2021-1976		
qcn5122					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5- 061021/1195
qcn5124					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCN5- 061021/1196
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1976		
qcn5152					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	ation of P2P PD Request gon Auto, bute, ectivity, amer IOT, strial IOT, & Music, ables, d d https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	
qcn5154			CVE ID : CVE-2021-1770		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCN5- 061021/1198
qcn5164					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcomm. com/compan y/product- security/bull	H-QUA-QCN5- 061021/1199
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976	etins/august -2021- bulletin	
qcn5500					
Use After Free	17-Sen-71			H-QUA-QCN5- 061021/1200	
qcn5502					
Use After Free	17-Sep-21	10	A use after free can occur du to improper validation of P2 device address in PD Reques frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan	H-QUA-QCN5- 061021/1201
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	h	NCII	PC ID
qcn5550							
Use After Free	17-Sep-21	10	A use after free can occur to improper validation of device address in PD Rec frame in Snapdragon Aut Snapdragon Compute, Snapdragon Connectivity Snapdragon Consumer IC Snapdragon Industrial IC Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-197	f P2P quest to, https://v w.qualco com/con y/produ security/ etins/au -2021- bulletin	omm. mpan ict- /bull	_	-QCN5- 1/1202
qcn6023							
Use After Free	17-Sep-21	10	A use after free can occur to improper validation of device address in PD Rec frame in Snapdragon Aut Snapdragon Compute, Snapdragon Connectivity Snapdragon Consumer IC Snapdragon Industrial IC Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-197	f P2P quest to, https://ww.qualco.com/com/com/oT, OT, security/etins/au -2021- bulletin			-QCN6- 1/1203
qcn6024							
Use After Free	17-Sep-21	10	A use after free can occur to improper validation of device address in PD Rec frame in Snapdragon Aut Snapdragon Compute, Snapdragon Connectivity Snapdragon Consumer IC Snapdragon Industrial IC	https://www.qualcomm.com/company/product-security/bulletins/august		_	-QCN6- 1/1204
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	bulletin	
qcn6122					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN6- 061021/1205
qcn9000					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCN9- 061021/1206
qcn9012					
Use After	17-Sep-21	10	A use after free can occur due	https://ww	H-QUA-QCN9-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/1207
qcn9022					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCN9- 061021/1208
qcn9024					
Use After Free	17-Sep-21	device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCN9- 061021/1209
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1976		
qcn9070					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN9- 061021/1210
qcn9072					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCN9- 061021/1211
qcn9074					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://ww w.qualcomm. com/compan	H-QUA-QCN9- 061021/1212
CVSS Scoring Sca	le 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976	y/product- security/bull etins/august -2021- bulletin	
qcn9100					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	
qcs2290					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS2- 061021/1214
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCS2- 061021/1215
qcs405					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4- 061021/1216
qcs410					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCS4- 061021/1217
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap everflow due to lack of input ommand size validation while handling beacon emplate update command rom HLOS in Snapdragon auto, Snapdragon Consumer OT, Snapdragon Industrial OT, Snapdragon IoT, snapdragon Mobile, snapdragon Wearables  EVE ID: CVE-2021-30261		H-QUA-QCS4- 061021/1218
qcs4290			0.2.2.0.2.2.0.2.0		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCS4- 061021/1219
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCS4- 061021/1220
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description	& CVE ID		Pat	ch	NCI	IPC ID
			Snapdragon Voice Snapdragon Western Snapdragon Wire Infrastructure and Networking  CVE ID: CVE-20	arables, red nd					
Improper Input Validation	17-Sep-21	7.2	Possible integer overflow due to command size v while handling between template updates from HLOS in Snauto, Snapdragor IOT, Snapdragor Snapdragon Mol Snapdragon Western Snapdragon Snapdragon Western Snapdragon Western Snapdragon Snapdrag	lack of inpralidation beacon e command apdragon on Consum Industrian IoT, bile, ce & Music	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin		_	A-QCS4- 1/1221	
			CVE ID : CVE-20	021-3026	1				
qcs603									
NULL Pointer Dereference	17-Sep-21	4.9	occurs due to im validation when preemption feat enablement is to Snapdragon Aut Snapdragon Con Snapdragon Con Snapdragon Con Snapdragon Ind	preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  w.qua com/o y/pro securi etins/ -2021 bullet		https:/ w.qual- com/cc y/prod securit etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	_	A-QCS6- 1/1222
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,			https://w.qualcom/com/co y/prod securit etins/a -2021-	comm. ompan luct- y/bull	_	A-QCS6- 1/1223
CVSS Scoring Sca	ale <b>0-1</b>	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
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	bulletin	
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCS6- 061021/1224
			CVE ID: CVE-2021-30261		
qcs605					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6- 061021/1225
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA-QCS6- 061021/1226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	-2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCS6- 061021/1227
qcs610					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCS6- 061021/1228
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://ww w.qualcomm. com/compan	H-QUA-QCS6- 061021/1229
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	y/product- security/bull etins/august -2021- bulletin		
qcs6125						
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	ernel graphics driver ecause of storing an invalid ointer in Snapdragon ompute, Snapdragon onnectivity, Snapdragon dobile, Snapdragon Vearables, Snapdragon Vired Infrastructure and https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCS6- 061021/1231	
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://ww w.qualcomm.	H-QUA-QCS6- 061021/1232	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	com/compan y/product- security/bull etins/august -2021- bulletin	
qcx315					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCX3- 061021/1233
Improper Input 17-Sep-21 7.2 Validation		Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QCX3- 061021/1234	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 448 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
qet4101					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QET4- 061021/1235
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QET4- 061021/1236
qrb5165					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QRB5- 061021/1237

5-6

6-7

7-8

8-9

9-10

2-3 3-4 4-5

1-2

0-1

CVSS Scoring Scale

Weakness	Publish Date	cvss	Descri	iption & CVE	ID	Pa	tch	NCI	IPC ID	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976			com/c	comm. ompan duct- ty/bull august	_	A-QRB5- 1/1238	
qsm8250										
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939			com/c	comm. ompan duct- ty/bull august	H-QUA QSM8- 06102		
qsw8573										
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables		occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, https://www.qualcomm.com/company/product-security/bull etins/august-2021-bulletin		curs due to improper lidation when the eemption feature ablement is toggled in apdragon Auto, apdragon Connectivity, apdragon Consumer IOT, apdragon Industrial IOT,		H-QUA QSW8 06102	
CVSS Scoring Sca	le <b>0-1</b>	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	
			CVE ID : CVE-2021-1939			
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- QSW8- 061021/1241	
Improper Input 17-Sep-21 Validation		7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://ww w.qualcomm. com/compan y/product- security/bull	H-QUA- QSW8- 061021/1242	
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	etins/august -2021- bulletin		
qualcomm21	5					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939		H-QUA-QUAL- 061021/1243	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QUAL- 061021/1244
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-QUAL- 061021/1245
sa415m					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA41- 061021/1246

2-3 3-4 4-5

1-2

0-1

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Infrastructure and Networking				
			CVE ID : CVE-2021-1976				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Consumer OT, Snapdragon Industrial OT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  Possible integer and heap the provided the provided that the provided to lack of input the provided that the		H-QUA-SA41- 061021/1247		
			CVE ID : CVE-2021-30261				
sa515m							
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SA51- 061021/1248		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SA51- 061021/1249		
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10		

Weakness	Publish Date	cvss	Descripti	on & CVE	ID	Pa	tch	NCI	IPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261						
ca6145n			CVE ID : CVE	-2021-30	0201				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer of occurs due to validation who preemption for enablement is Snapdragon of Snapdragon o	improperien the eature stoggled Auto, Compute, Connective Consumer and warable	in vity, r IOT, l IOT,	_	comm. ompan luct- cy/bull august	_	A-SA61- 1/1250
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976			_	comm. ompan luct- cy/bull august	_	A-SA61- 1/1251
Improper Input Validation	17-Sep-21	7.2	overflow due command size while handlin template upd from HLOS in	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon  Auto, Snapdragon Consumer https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021-		_	A-SA61- 1/1252		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description &	CVE ID	Patch	n	NCI	PC ID
			IOT, Snapdragon In IOT, Snapdragon Mobil Snapdragon Voice Snapdragon Wears CVE ID: CVE-202	oT, e, & Music, ables	bulletin			
sa6150p								
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereft occurs due to improvalidation when the preemption featurenablement is togge Snapdragon Auto, Snapdragon Composition Snapdragon Connections Snapdragon Industry Snapdragon Weard	roper e e gled in ute, ectivity, mer IOT, trial IOT,	https://w.qualco com/com y/produ security/ etins/au -2021- bulletin	omm. npan ct- /bull	_	a-SA61- 1/1253
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		https://w w.qualco com/con y/produ security/ etins/au -2021- bulletin	omm. npan ct- /bull	_	a-SA61- 1/1254
Improper Input Validation	17-Sep-21	7.2	Possible integer ar overflow due to la command size vali while handling bea template update co	erflow due to lack of input erflow due to lack of input mmand size validation nile handling beacon mplate update command om HLOS in Snapdragon https://www.qualcomm. com/compan y/product-security/bull etins/august		H-QUA-SA61- 061021/1255		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-	5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	-2021- bulletin	
sa6155					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SA61- 061021/1256
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SA61- 061021/1257
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://ww w.qualcomm. com/compan y/product- security/bull	H-QUA-SA61- 061021/1258

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	etins/august -2021- bulletin	
sa6155p					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SA61- 061021/1259
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SA61- 061021/1260
Improper Input Validation  CVSS Scoring Sca	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon  2-3 3-4 4-5 5-6	https://ww w.qualcomm. com/compan y/product-	H-QUA-SA61- 061021/1261 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	security/bull etins/august -2021- bulletin	
sa8145p					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81- 061021/1262
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81- 061021/1263
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://ww w.qualcomm.	H-QUA-SA81- 061021/1264
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	com/compan	8-9 <b>9-10</b>

Weakness	Publish Date	cvss	Description & CVE ID		Pat	ch	NCI	IPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consum IOT, Snapdragon Industria IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music Snapdragon Wearables  CVE ID: CVE-2021-3026	ner al c,	y/prod security etins/a -2021- bulletin	y/bull ugust		
sa8150p								
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939		https://w.qualocom/com/com/com/com/com/com/com/com/com	comm. ompan uct- y/bull ugust	_	A-SA81- 1/1265
Use After Free	17-Sep-21	10	A use after free can occur to improper validation of device address in PD Requireme in Snapdragon Auto Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IO Snapdragon Industrial IO Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://w.qualcom/com/co y/prod/security etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	_	A-SA81- 1/1266	
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of inp		https:// w.qualo		_	A-SA81- 1/1267
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5</b>	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	com/compan y/product- security/bull etins/august -2021- bulletin	
sa8155					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81- 061021/1268
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P21 device address in PD Reques frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	P	H-QUA-SA81- 061021/1269
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	H-QUA-SA81-
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/1270
sa8155p					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81- 061021/1271
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SA81- 061021/1272
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SA81- 061021/1273
sa8195p					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SA81- 061021/1274
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SA81- 061021/1275
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 462 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pa	tch	NCI	IPC ID
			CVE ID	: CVE-2	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	overflocomma while he templated from He Auto, Son IOT, Son Son Son Son Son Son Son Son Son Son	ow due to and size handling ite upda (LOS in S napdrag hapdrag hapdrag ragon W ragon W	obile, oice & M 'earable	f input on nand gon sumer strial	com/c	comm. ompan luct- cy/bull august	_	A-SA81- 1/1276
			CVE ID	CVE ID : CVE-2021-30261						
sc8180x\\+sc	dx55									
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261		com/c	comm. ompan luct- cy/bull august	_	A-SC81- 1/1277		
sd205										
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,		to improper when the w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin		comm. ompan duct- cy/bull august	n H-QUA-SD20- 061021/1278		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descript	ion & CVE	ID	Pa	tch	NCI	IPC ID
			Snapdragon V	Wearable	S				
			CVE ID : CVE	-2021-19	939				
Use After Free	17-Sep-21	10	device address frame in Snap Snapdragon ( Snapdragon ( Snapdragon I Snapdragon I Snapdragon I Snapdragon I Snapdragon I	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976				_	A-SD20- :1/1279
			CVE ID : CVE	-2021-19	976				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261		•	comm. ompan duct- cy/bull august	_	A-SD20- :1/1280	
sd210									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		H-QUA-SD21- 061021/1281		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables		
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD21- 061021/1282
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD21- 061021/1283
sd429					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD42- 061021/1284
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD42- 061021/1285
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD42- 061021/1286
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD42- 061021/1287
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 466 of 861	6-7 7-8	8-9 9-10

Pointer Dereference  17-Sep-21  4.9  Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,	LL nter 1			Snapdragon Voice & Music, Snapdragon Wearables  CVE ID : CVE-2021-30261  Null pointer dereference occurs due to improper		
NULL Pointer Dereference  17-Sep-21  17-Sep-21  A.9  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired  17-Sep-21  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Compute, Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired	LL nter 1			Null pointer dereference occurs due to improper		
NULL Pointer Dereference  17-Sep-21  Use After Free  17-Sep-21  Pointer Free  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Compute, Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired	LL nter 1			occurs due to improper		
Use After Free  17-Sep-21  To improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, https://www.qualcomm. com/compan y/product-security/bull of the property of the proper		17-Sep-21	4.9	preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-SD43- 061021/1288
Networking  CVE ID : CVE-2021-1976	1	17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-SD43- 061021/1289
Innif   1/-Sen-/  // Williams Season   1/-	-	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-SD43- 061021/1290

Weakness	Publish Date	cvss	Description & C\	'E ID	Pat	ch	NCI	IPC ID	
			IOT, Snapdragon IoT Snapdragon Mobile, Snapdragon Voice & Snapdragon Wearab	Music, les					
1450			CVE ID : CVE-2021-	30261					
sd450			N. 11		1		-		
NULL Pointer Dereference	17-Sep-21	4.9	validation when the preemption feature enablement is toggle Snapdragon Auto, Snapdragon Comput Snapdragon Connect Snapdragon Consum Snapdragon Industr	preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939		/ww comm. ompan luct- y/bull nugust	_	A-SD45- 1/1291	
			CVE ID : CVE-2021-	1939					
Use After Free	17-Sep-21	10	A use after free can of to improper validating device address in PE frame in Snapdragon Snapdragon Computed Snapdragon Connect Snapdragon Consum Snapdragon Industry Snapdragon Wearab Snapdragon Wearab Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-	https:/ w.qualcom/co y/prod securit etins/a -2021- bulletin	comm. compan luct- y/bull nugust	_	A-SD45- :1/1292		
Improper Input Validation	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon w.o.		overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon w.qualcom com/compy/product y/product security/kg etins/aug		comm. compan luct- y/bull lugust	_	A-SD45- 1/1293
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	bulletin	
sd460					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD46- 061021/1294
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD46- 061021/1295
sd480					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature	https://ww w.qualcomm. com/compan y/product-	H-QUA-SD48- 061021/1296

**2-3 3-4 4-5** 

1-2

0-1

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			enablement is Snapdragon A Snapdragon C Snapdragon C Snapdragon Ir Snapdragon W CVE ID: CVE-	uto, ompute, onnectiv onsumen dustrial	ity, · IOT, IOT, s	securit etins/a -2021- bulleti	august		
			A use after fre						
Use After Free	17-Sep-21	10	to improper volume to improper volume address frame in Snape Snaperagon C Snaperagon C Snaperagon In Snaperagon W Snaperagon W Snaperagon W Snaperagon W Infrastructure Networking  CVE ID: CVE-	alidations in PD R dragon A ompute, onnective onsumendustrial foice & M Vearable Vired	equest Auto, ity, IOT, IOT, usic, s,	https:/ w.qual com/c y/prod securit etins/a -2021- bulleti	comm. compan luct- cy/bull nugust	_	SD48- 1/1297
			Possible integ						
Improper Input Validation	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			https:/ w.qual com/c y/prod securit etins/a -2021- bulleti	comm. compan luct- y/bull nugust	_	SD48- 1/1298
sd632						1		1	
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer d occurs due to validation who	_	/ww comm. ompan	_	-SD63- 1/1299		
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			enable Snapd Snapd Snapd Snapd Snapd Snapd	aption feement is ragon Caragon Caragon Caragon Caragon Was and the ragon Was and the Core and the ragon Was and the core	toggled uto, ompute, onnectiv onsume ndustrial	rity, r IOT, IOT, s	y/prod securit etins/a -2021- bulleti	ty/bull august		
Use After Free	17-Sep-21	10	to impose devices frame Snapd Snapd Snapd Snapd Snapd Infrast Netwo	after fre proper value address in Snape ragon C ragon C ragon V ragon W ragon W tructure orking  D: CVE-	alidations in PD F dragon A ompute, onnective onsume ndustrial oice & M Vearable Vired and	a of P2P dequest Auto, rity, r IOT, IOT, fusic, s,	com/c	comm. ompan luct- cy/bull august	_	A-SD63- 1/1300
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261				https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin			A-SD63- 1/1301
sd660										
Use After Free	17-Sep-21	7.2		ter-free I graphic		•	https://ww w.qualcomm.		_	A-SD66- 31/1302
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	com/compan y/product- security/bull etins/august -2021- bulletin	
1000			CVE ID : CVE-2021-1947		
sd662					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD66- 061021/1303
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD66- 061021/1304
sd665					

NULL Pointer Dereference  17-Sep-21  17-Sep-21  18-9  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Wearables CVE ID : CVE-2021-1939  Use After Free  17-Sep-21  Use After Free  17-Sep-21  17-Sep-21  17-Sep-21  Use After Free  17-Sep-21  17-Sep-21  18-9  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wearables, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Nobile, Snapdragon Wearables, Snapdragon Connectivity, Snapdragon Conpute, Snapdragon Conpute, Snapdragon Conpute, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Auto, Snapdragon Conpute, Snapdragon Conpute, Snapdragon Conpute, Snapdragon Conpute, Snapdragon Conpute, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Conpute, Snapdrago	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
See After Free   17-Sep-21   10	Pointer	17-Sep-21	4.9	occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	_
Use After Free  17-Sep-21  10  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, https://www.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin		17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	_
45.0 04 50		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	_
r -r -	Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	H-QUA-SD66-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/1308
sd670					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67- 061021/1309
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD67- 061021/1310
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD67- 061021/1311
sd675					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD67- 061021/1312
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD67- 061021/1313
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	n & CVE	ID	Pa	tch	NCI	PC ID
			Netwo	rking						
			CVE II	) : CVE-2	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	overflocommon while templatemp	le intege ow due t and size handling ate upda ILOS in S Snapdrag napdrag napdrag ragon W ragon W	o lack o validati s beacor te comm Snapdra gon Con on Indu on IoT, obile, pice & M Yearable	f input on nand gon sumer strial lusic, s	com/c y/pro securi	comm. compan duct- ty/bull august	_	A-SD67- 1/1317
sd690_5g				_						
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables				com/c y/pro securi	comm. compan duct- ty/bull august	_	A-SD69- 1/1318
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			com/c y/pro securi	comm. compan duct- ty/bull august		a-SD69- 1/1319	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Free 17-Sep-21 19 Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976 Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261 Sd712  Improper Input 17-Sep-21 Ty-Sep-21 Ty-Sep-21 Validation 17-Sep-21 Ty-Sep-21 Validation 17-Sep-21 Ty-Sep-21 Ty-Se	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking  Improper Input Validation  Improper Input Validation				CVE ID : CVE-2021-1947			
Improper Input Validation  Validation  Improper Input Validation  Improper		Use After Free 17-Sep-21 10		to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-SD69- 061021/1320	
Improper Input Validation  To Sep-21 Validation  Improper Input Validation  Improper Input Validation  Input Validation  To Sep-21  Input Validation  Input Validation  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,  Possible integer and heap overflow due to lack of input w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	Input	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-SD69- 061021/1321	
Improper Input Validation  17-Sep-21  Total Parameters overflow due to lack of input command size validation with with and ling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,  Auto Snapdragon Industrial to Total Parameters overflow due to lack of input with under the properties of the prop	sd712						
Shaparagon Probincy	Input	mproper nput Validation  17-Sep-21  7.2  Possible integer ar overflow due to la command size vali while handling beat template update of from HLOS in Snap Auto, Snapdragon IOT, Snapdragon IO		overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-SD71- 061021/1322	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music,		
			Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
sd720g					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD72- 061021/1323
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD72- 061021/1324
sd730					
NULL Pointer 17-Sep-2 Dereference		4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA-SD73- 061021/1325

6-7

7-8

8-9

9-10

2-3 3-4 4-5

1-2

0-1

Weakness	Publish Date	cvss	Desc	cription & C\	'E ID	Pa	tch	NCI	IPC ID
			Snapdrag Snapdrag Snapdrag Snapdrag	on Comput on Connect on Consum on Industr on Wearab	civity, er IOT, al IOT, les	-2021- bulleti			
Use After Free	17-Sep-21	10	device ad frame in S Snapdrag Snapdrag Snapdrag Snapdrag Snapdrag Snapdrag Infrastruc Networki	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap				_	A-SD73- :1/1326
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			https:/ w.qual com/c y/proc securit etins/a -2021- bulleti	comm. ompan luct- cy/bull august	_	A-SD73- 1/1327
sd750g									
NULL Pointer Dereference	17-Sep-21	4.9	Null poin occurs du validation preempti enableme	com/c	comm. ompan	H-QUA-SD75- 061021/1328			
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	etins/august -2021- bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD75- 061021/1329
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD75- 061021/1330
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA-SD75- 061021/1331
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 Page 481 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descript	ion & CVE	ID	Pat	tch	NCI	IPC ID
			Auto, Snapdra IOT, Snapdra IOT, Snapdra Snapdragon Snapdragon Snapdragon	gon Indu gon IoT, Mobile, Voice & M Wearable	strial Iusic, s	-2021- bulleti			
sd765									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer occurs due to validation where the content of the con	o improper nen the Seature s toggled Auto, Compute, Connectiv Consumer Industrial	in vity, r IOT, l IOT, s	_	comm. compan luct- cy/bull nugust	_	A-SD76- 1/1332
Use After Free	17-Sep-21	7.2	Use-after-fre kernel graph because of st pointer in Sn Compute, Sn Connectivity Industrial IO Mobile, Snap Wearables, S Wired Infras Networking	alid https://v w.qualco com/com y/produc security/ etins/aug -2021- bulletin		_	A-SD76- 1/1333		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P w.qualcomm. device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, https://www.qualcomm. com/compan y/product-security/bull etins/august -2021-			_	A-SD76- 1/1334		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

<b>Publish Date</b>	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	bulletin	
		CVE ID : CVE-2021-1976		
17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD76- 061021/1335
		CVE ID: CVE-2021-30261		
17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76- 061021/1336
			https://www	
17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA-SD76- 061021/1337
	17-Sep-21	17-Sep-21 4.9	Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-30261  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wearables CVE ID: CVE-2021-1939  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Compute, Snapdragon	Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables CVE ID: CVE-2021-30261  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Consumer IOT, Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID: CVE-2021-30261  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mearables CVE ID: CVE-2021-1939  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon

Weakness	Publish Date	CVSS	De	scriptio	n & CVE	ID	Pa	tch	NCI	IPC ID		
			Industri Mobile, Wearab Wired In Networl	Snapdr les, Sna nfrastr king	ragon apdrago ucture a	on and	-2021- bulleti					
Use After Free	17-Sep-21	10	Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976				_	comm. ompan luct- y/bull nugust	_	A-SD76- 21/1338		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261				https:/ w.qual com/c y/proc securit etins/a -2021- bulleti	comm. compan luct- cy/bull nugust	_	A-SD76- 21/1339		
sd768g												
NULL Pointer Dereference	17-Sep-21	4.9	occurs of validation preemp enablem	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in			occurs due to improper w.qualcomm. validation when the com/compan preemption feature y/product-			1 061021/1340 I		
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	etins/august -2021- bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD76- 061021/1341
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD76- 061021/1342
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA-SD76- 061021/1343
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 485 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	-2021- bulletin	
sd778g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD77- 061021/1344
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD77- 061021/1345
Improper Input Validation  CVSS Scoring Sca	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://ww w.qualcomm. com/compan y/product- security/bull	H-QUA-SD77- 061021/1346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	etins/august -2021- bulletin	
sd780g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD78- 061021/1347
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD78- 061021/1348
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://ww w.qualcomm. com/compan y/product-	H-QUA-SD78- 061021/1349

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	security/bull etins/august -2021- bulletin	
sd820					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD82- 061021/1350
sd821					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD82- 061021/1351
sd835					

CVSS Scoring Scale

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD83- 061021/1352
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD83- 061021/1353
sd845					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD84- 061021/1354
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 489 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD84- 061021/1355
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD84- 061021/1356
sd850					
Improper Input Validation	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon IoT,		overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD85- 061021/1357
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 490 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
				lragon V						
				lragon W						
1055			CVE	D : CVE-	2021-3	0261				
sd855			NT 11	• • •			I		Τ	
NULL Pointer Dereference	17-Sep-21	4.9	valida preem enable Snapd Snapd Snapd Snapd Snapd	occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939 Use-after-free vulnerability in kernel graphics driver				//ww comm. ompan duct- ty/bull august	_	A-SD85- 1/1358
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking				_	comm. ompan duct- ty/bull august	_	A-SD85- 1/1359
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired			•	comm. ompan duct- ty/bull august	H-QUA-SD85-		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Par	tch	NCI	IPC ID
			Infrast Netwo	ructure rking	and					
			CVE II	) : CVE-2	2021-1	976				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261				_	comm. compan luct- cy/bull nugust	_	A-SD85- 21/1361
			CVE II	) : CVE-	2021-3	0261				
sd865_5g										
NULL Pointer Dereference	17-Sep-21	4.9	preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,				_	comm. ompan luct- y/bull nugust	_	A-SD86- 21/1362
Use After Free	17-Sep-21	7.2	kernel becaus pointe Compu Conne Indust Mobile Weara	ter-free graphic se of sto r in Sna ite, Snap ctivity, S rial IOT e, Snapd bles, Sna	es driver ring an i pdragor odragon Snapdra , Snapdr ragon apdrago	invalid n gon ragon		comm. compan luct- cy/bull nugust		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Descripti	on & CVE	ID	Pa	tch	NCI	IPC ID
			Networking						
			CVE ID : CVE-	2021-19	947				
Use After Free	17-Sep-21	10	to improper volume device address frame in Snap Snapdragon Constitution of Snapdragon Consportation of Snapdragon Volume Snapdragon S	se after free can occur due in proper validation of P2P ice address in PD Request in En Snapdragon Auto, pdragon Compute, pdragon Connectivity, pdragon Consumer IOT, pdragon Industrial IOT, pdragon Wearables, pdragon Wired astructure and working			//ww comm. ompan duct- cy/bull august	_	A-SD86- 21/1364
			CVE ID : CVE-	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	overflow due command size while handlin template upda from HLOS in Auto, Snapdrag IOT, Snapdrag Snapdragon M Snapdragon W Snapdragon W Snapdragon W	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  EVE ID: CVE-2021-30261			//ww comm. ompan luct- cy/bull august	_	A-SD86- 21/1365
sd870				2021 30201					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,			com/c	comm. ompan luct- cy/bull august	H-QUA-SD87- 061021/1366	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables		
			CVE ID: CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD87- 061021/1367
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD87- 061021/1368
Improper Input Validation	Possible integer and heap overflow due to lack of inpur command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT,		overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD87- 061021/1369

**2-3 3-4 4-5** 

1-2

0-1

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		
			CVE ID : CVE-2021-30261		
sd888					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD88- 061021/1370
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD88- 061021/1371
sd888_5g					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-SD88- 061021/1372
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 495 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description	ption & CVE ID		Pat	ch	NCI	IPC ID
			Snapdragon C Snapdragon C Snapdragon Ir Snapdragon W CVE ID: CVE-	onsume Idustrial Jearable	r IOT, I IOT, s	bulletii	1		
Use After Free	17-Sep-21	10	A use after free to improper volume address frame in Snaperagon Consumer Snaperagon Consumer Snaperagon Volume Snaperagon Work	tructure and orking  D: CVE-2021-1976  ole integer and heap		comm. ompan uct- y/bull ugust	_	A-SD88- 1/1373	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			https:/ w.qualcom/co y/prod securit etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	_	A-SD88- 1/1374
sda429w									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,			https:/ w.qualcom/co y/prod securit etins/a	comm. ompan uct- y/bull	H-QUA-SDA4- 061021/1375	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Use After Free 17-Sep-21 7.2 Improper Input Validation 17-Sep-21 7.2 Sdm429w	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939 Use-after-free vulnerability in	-2021- bulletin	
Use After Free 17-Sep-21 7.2 Improper Input Validation 17-Sep-21 7.2 Sdm429w	Use-after-free vulnerability in		
Improper Input 17-Sep-21 7.2 Validation	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SDA4- 061021/1376
	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SDA4- 061021/1377
NULL Pointer Dereference  CVSS Scoring Scale  17-Sep-21 4.9  CVSS Scoring Scale  17-Sep-21 4.9  17-Sep-21 4.9  17-Sep-21 4.9  17-Sep-21 4.9	Null pointer dereference occurs due to improper	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA- SDM4- 061021/1378

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- SDM4- 061021/1379
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- SDM4- 061021/1380
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- SDM4- 061021/1381

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261		
sdm630					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- SDM6- 061021/1382
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- SDM6- 061021/1383
sdm830					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature	https://ww w.qualcomm. com/compan y/product-	H-QUA- SDM8- 061021/1384

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID				Pat	ch:	NCI	IPC ID
			enablem Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra	igon Au igon Co igon Co igon Co igon Ind	ito, impute, innectiv insume dustrial	rity, r IOT, l IOT,	securit etins/a -2021- bulletin	ugust		
			CVE ID:	CVE-2	021-19	939				
Use After Free	17-Sep-21	7.2	Use-afte kernel g because pointer i Compute Connect Industri Mobile, S Wearabl Wired In Network	raphics of stor in Snap e, Snap ivity, S al IOT, Snapdr les, Sna nfrastru king	s driver ing an i dragon dragon napdra Snapdr agon apdrago	nvalid gon agon n	https:/ w.qual com/co y/prod securit etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	H-QUA SDM8 06102	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976			https:/ w.qual com/co y/prod securit etins/a -2021- bulletin	comm. compan uct- y/bull ugust	H-QUA SDM8 06102		
sdw2500										
Use After Free	17-Sep-21	10	to impro device a	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,			https:/ w.qual com/co y/prod	comm. ompan	H-QUA SDW2 06102	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	ı	Description	escription & CVE ID		Pa	tch	NCI	IPC ID
			Snapd Snapd Snapd Snapd Snapd Infrasi	Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap				ty/bull august n		
Improper Input Validation	17-Sep-21	7.2	overflocomm while temple from I Auto, S IOT, St Snapd Snapd Snapd	ole intego ow due t and size handling ate upda HLOS in S Snapdrag napdrag napdrag ragon M ragon W	to lack of validating beacon te common to the common to the contraction on IoT, to bile, to bice & Marable	f input ion n mand agon ssumer strial fusic,	com/c y/prod securi	comm. compan duct- ty/bull august	H-QUA SDW2 06102	
sdx12										
Use After Free	17-Sep-21	10	to impose devices frame Snapd Snapd Snapd Snapd Snapd Infrast Netwo	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		com/c y/prod securi	comm. compan duct- ty/bull august	_	A-SDX1- 21/1389	
Improper	17-Sep-21	7.2	Possib	ole intege	er and h	eap	https:/	//ww	H-QU	A-SDX1-
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/1390
sdx20					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2- 061021/1391
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SDX2- 061021/1392

**2-3 3-4 4-5** 

1-2

0-1

5-6

6-7

8-9

9-10

7-8

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			CVE II	D : CVE-	2021-30	)261				
sdx20m										
Use After Free	17-Sep-21	10	to impose devices frame Snapd Snapd Snapd Snapd Snapd Infras	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			_	comm. ompan luct- cy/bull august	_	A-SDX2- 21/1393
			CVE II	CVE ID : CVE-2021-1976						
sdx24										
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables		com/c	comm. ompan luct- cy/bull august		A-SDX2- 21/1394	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,			com/c	comm. ompan luct- cy/bull august	_	A-SDX2- 21/1395	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description	scription & CVE ID			ch	NCI	PC ID
			Snapdragon Wi Infrastructure a Networking						
			CVE ID : CVE-2	021-1976	)				
Improper Input Validation	17-Sep-21	7.2	overflow due to command size v while handling template update from HLOS in St Auto, Snapdrago IOT, Snapdrago IOT, Snapdrago Snapdragon Mo Snapdragon We Snapdragon We	ersible integer and heap verflow due to lack of input mmand size validation hile handling beacon mplate update command om HLOS in Snapdragon ito, Snapdragon Consumer T, Snapdragon Industrial T, Snapdragon IoT, sapdragon Mobile, sapdragon Wearables VE ID: CVE-2021-30261			/ww comm. ompan uct- y/bull ugust	_	a-SDX2- 1/1396
sdx50m									
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		https:/ w.qual- com/co y/prod securit etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	_	A-SDX5- 1/1397	
Improper Input Validation	17-Sep-21	7.2	Possible integer overflow due to command size while handling template update from HLOS in Stranger Auto, Snapdrag	https://w.qualcom/co y/prod securit etins/a -2021-	comm. ompan uct- y/bull	_	a-SDX5- 1/1398		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	bulletin	
sdx55					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5- 061021/1399
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947		H-QUA-SDX5- 061021/1400
Use After Free	17-Sep-21	10	A use after free can occur du to improper validation of P2 device address in PD Reques frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SDX5- 061021/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		
			Possible integer and heap overflow due to lack of input command size validation		
Improper Input Validation	17-Sep-21	7.2	while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SDX5- 061021/1402
sdx55m			CVE ID : CVE-2021-30261		
SuxJJIII			Null nointer dereference		
NULL Pointer Dereference	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IO' Snapdragon Industrial IO'		occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SDX5- 061021/1403
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-SDX5- 061021/1404

Weakness	Publish Date	cvss	Description	on & CVE	ID	Pat	ch	NCI	IPC ID
			Mobile, Snapd Wearables, Sn Wired Infrastr Networking CVE ID: CVE-	apdrago ucture a	and	bulletii	1		
Use After Free	17-Sep-21	10	A use after fre to improper ve device address frame in Snape Snapdragon C Snapdragon C Snapdragon In Snapdragon V Snapdragon W Snapdragon W Infrastructure Networking CVE ID : CVE-	https:/ w.qualcom/co y/prod securit etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	_	A-SDX5- 1/1405		
Improper Input Validation	17-Sep-21	7.2	Possible integoverflow due for command size while handling template update from HLOS in Auto, Snapdrag IOT, Snapdrag Snapdragon Manapdragon Washapdragon Washapdr	https:/ w.qualcom/co y/prod securit etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	_	A-SDX5- 1/1406		
sdxr1									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,			https:/ w.qualcom/co y/prod securit etins/a	comm. ompan uct- y/bull	H-QUA-SDXR- 061021/1407	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Des	cription 8	& CVE	ID	Pa	tch	NCI	IPC ID
			Snapdrag Snapdrag Snapdrag Snapdrag Snapdrag	gon Conr gon Cons gon Indu gon Wea	nectiv sumer strial rable	· IOT, IOT, s	-2021- bulleti			
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap				_	comm. ompan luct- cy/bull august	_	A-SDXR- 21/1408
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261				https:/ w.qual com/c y/proc securit etins/a -2021- bulleti	comm. ompan luct- cy/bull august	_	A-SDXR- 21/1409
sdxr2_5g										
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in					comm. ompan luct-	_	A-SDXR- 21/1410
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descr	iption & CVE	ID	Pat	ch	NCI	IPC ID
			Snapdrago Snapdrago Snapdrago Snapdrago	n Auto, n Compute, n Connectiv n Consume n Industrial n Wearable	· IOT, · IOT, · s	etins/a -2021- bulletin			
Use After Free	17-Sep-21	10	A use after to imprope device add frame in Si Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Infrastruct Networkin	https:/ w.qual com/co y/prod securit etins/a -2021- bulletin	comm. compan luct- y/bull lugust	_	A-SDXR- 21/1411		
Improper Input Validation	17-Sep-21	7.2	Possible in overflow d command while hand template u from HLOS Auto, Snap IOT, Snap d IOT, Snap d Snap drago Snap drago Snap drago CVE ID: C	https:/ w.qual com/co y/prod securit etins/a -2021- bulletin	comm. compan luct- y/bull lugust		A-SDXR- 21/1412		
sd_455									
Use After Free	17-Sep-21	10	A use after to imprope device add frame in Si	https:/ w.qual com/co y/prod	comm. ompan	_	A-SD_4- 21/1413		
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-	4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD_4- 061021/1414
sd_636					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SD_6- 061021/1415
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	H-QUA-SD_6-
CVSS Scoring Sca	ile 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Input Validation Valid	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference  17-Sep-21  Use After Free  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  Null pointer dereference occurs due to improper validation when the preemption feature w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin  H-QUA-SD_6-061021/1417  H-QUA-SD_6-061021/1418  etins/august -2021-bulletin	-			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	com/compan y/product- security/bull etins/august -2021-	061021/1416
NULL Pointer Dereference  17-Sep-21  Use After Free  17-Sep-21  10  Occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  NULL  H-QUA-SD_6-061021/1418	sd_675					
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	Pointer	17-Sep-21	4.9	occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	_
		17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	_

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Snapd	ragon W	/earable	S				
			CVE II	D : CVE-	2021-3	0261				
sm4125							1			
NULL Pointer Dereference	17-Sep-21	4.9	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  security/bull etins/august -2021- bulletin		ht dation when the emption feature ablement is toggled in apdragon Auto, apdragon Compute, apdragon Consumer IOT, apdragon Industrial IOT, apdragon Wearables  E ID : CVE-2021-1939  e-after-free vulnerability in				_	A-SM41- 21/1422
Use After Free	17-Sep-21	7.2	kernel becau pointe Comp Conne Indust Mobile Weara Wired Netwo	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947				//ww comm. ompan duct- ty/bull august		A-SM41- 21/1423
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and				com/c y/prod securi	comm. ompan duct- ty/bull august		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Networking			
			CVE ID : CVE-2021-1976			
sm6250						
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SM62- 061021/1425	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62- 061021/1426	
sm6250p	•					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	H-QUA-SM62- 061021/1427	

2-3 3-4 4-5

1-2

0-1

5-6

6-7

7-8

8-9

9-10

Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	bulletin	
		CVE ID : CVE-2021-1976		
17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SM62- 061021/1428
		CVE ID: CVE-2021-30261		
17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA-SM72- 061021/1429
			httma.//	
17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	H-QUA-SM72- 061021/1430
	17-Sep-21	17-Sep-21 7.2 17-Sep-21 4.9	Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-30261  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Compute, Snapdragon	Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon IoT, Snapdragon Mobile, Snapdragon Nobile, Snapdragon Wearables CVE ID: CVE-2021-30261  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Wearables CVE ID: CVE-2021-1939  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Compute

Weakness	Publish Date	cvss	De	scriptio	n & CVE	ID	Pa	tch	NCI	IPC ID
			Industri Mobile, S Wearabl Wired Ir Network	Snapdr les, Sna nfrastru king	ragon ipdrago ucture a	on and	-2021- bulleti			
Use After Free	17-Sep-21	10	A use aft to impro device a frame in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra CVE ID:	oper valdress Snapd gon Co gon Co gon In gon W gon W ucture king	lidatior in PD F lragon A ompute, onsume dustrial oice & M earable ired and	n of P2P Request Auto, vity, r IOT, I IOT, Iusic, s,	_	comm. ompan luct- cy/bull nugust	_	A-SM72- 21/1431
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261				https:/ w.qual com/c y/prod securit etins/a -2021- bulleti	comm. ompan luct- cy/bull august	_	A-SM72- 21/1432
sm7325										
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in				com/c y/proc securit	comm. ompan luct- cy/bull	06102	A-SM73- 21/1433
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	etins/august -2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM73- 061021/1434
wcd9306	<u>,                                      </u>				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1435
wcd9326					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver	https://ww w.qualcomm.	H-QUA- WCD9-
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 517 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	com/compan y/product- security/bull etins/august -2021- bulletin	061021/1436
wcd9330	1			1	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCD9- 061021/1437
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1438
wcd9335					
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1439	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1440	
wcd9340	L					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9-	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver	https://ww w.qualcomm.	H-QUA- WCD9-	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	com/compan y/product- security/bull etins/august -2021- bulletin	061021/1442
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1443
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1444
wcd9341					
Use After	17-Sep-21	7.2	Use-after-free vulnerability in	https://ww	H-QUA-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID					
Free			kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	WCD9- 061021/1445					
wcd9360										
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCD9- 061021/1446					
wcd9370										
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1447					

CVSS Scoring Scale

5-6

8-9

7-8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1448
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1449
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1450

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
wcd9371					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1451
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCD9- 061021/1452
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1453
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 523 of 861	6-7 7-8	8-9 <b>9-10</b>

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			CVE II	) : CVE-	2021-30	0261				
wcd9375									L	
NULL Pointer Dereference	17-Sep-21	4.9	occurs validat preem enable Snapd Snapd Snapd Snapd Snapd Snapd	tion who ption fe ement is ragon Co ragon Co ragon Co ragon In	ature toggled uto, ompute, onnectiv onsume idustrial	in vity, r IOT, I IOT, s	com/c y/prod securit	comm. ompan duct- ty/bull august	H-QUA WCD9 06102	
	CVE ID : CVE-2021-1939									
Use After Free	17-Sep-21	7.2	kernel becaus pointe Compu Conne Indust Mobile Weara Wired Netwo	graphicse of store in Snapetivity, Strial IOT, e, Snapetiles, Snap	es driver ring an i pdragon odragon Snapdra , Snapdr	nvalid gon ragon n	com/c y/prod securit	comm. ompan duct- ty/bull august	H-QUA WCD9 06102	
Use After Free	17-Sep-21	10	to imp device frame Snapd Snapd Snapd Snapd Snapd Snapd Snapd	roper va address in Snapo ragon Co ragon Ir ragon V ragon W ragon W		of P2P Request Auto, vity, r IOT, I IOT,	com/c y/prod securit	comm. ompan duct- ty/bull august		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	(	Description	on & CVE	ID	Pa	itch	NCI	IPC ID
			CVE II	O : CVE-	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	overflocomm while templa from I Auto, S IOT, Si Snapd Snapd Snapd	ow due to and size thandling ate update and	to lack of validating beacon ite common induration on IoT, lookie, when items is to be a constant on IoT, which is to be a constant in the interval of the int	f input ion nand igon sumer strial lusic, s	com/o y/pro securi	comm. compan duct- ty/bull august	H-QU/ WCD9 06102	
wcd9380										
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	ointer designation who interest of the interes	imprope en the ature toggled uto, ompute, onnectiv onsume idustria	in vity, r IOT, I IOT, s	com/o y/pro securi	comm. compan duct- ty/bull august	H-QU/ WCD9 06102	
Use After Free	17-Sep-21	7.2	kernel becaus pointe Compt Conne Indust Mobile Weara Wired Netwo	graphicse of sto or in Snaute, Snap ctivity, Strial IOT e, Snapd lbles, Sn Infrastr	es driver ring an i pdragon Snapdra , Snapdr ragon apdrago	nvalid gon ragon on	com/o y/pro securi	comm. compan duct- ty/bull august	H-QUA WCD9 06102	
	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
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCD9- 061021/1460
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1461
wcd9385					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1462
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1463
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1464
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCD9- 061021/1465

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			CVE II	CVE-	2021-30	0261				
wcn3610										
NULL Pointer Dereference	17-Sep-21	4.9	occurs validat preem enable Snapd Snapd Snapd Snapd Snapd Snapd	tion who ption fe ement is ragon Ca ragon Ca ragon Ca ragon Ir ragon W	ature toggled uto, ompute, onnectiv onsume idustrial	in vity, r IOT, I IOT, s	com/c y/prod securi	comm. compan duct- ty/bull august	H-QUA WCN3 06102	
	CV				2021-19	939				
Use After Free	17-Sep-21	7.2	kernel becaus pointe Compu Conne Indust Mobile Weara Wired Netwo	graphicse of sto r in Snaute, Snap ctivity, S rial IOT e, Snapd bles, Sn Infrastr	es driver ring an i pdragon odragon Snapdra	nvalid gon ragon on	com/c y/prod securi	comm. compan duct- ty/bull august	H-QUA WCN3 06102	
Use After Free	17-Sep-21	10	to imp device frame Snapd Snapd Snapd Snapd Snapd Snapd Snapd	roper va address in Snape ragon Co ragon Ir ragon V ragon W ragon W	s in PD F dragon A ompute, onnective onsume dustrial oice & M Vearable Vired	of P2P Request Auto, vity, r IOT, I IOT,	com/c y/prod securi	comm. compan duct- ty/bull august		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					tch	NCI	IPC ID
			CVE II	O : CVE-	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	overflocomm while templated from H Auto, Standard, Standard Snapd Snapd	ow due to and size thandling ate update and andrag napdrag ragon Wragon Wragon W	to lack of validating beacon ite common induration on IoT, lookie, when items is to be a rable of the contract	f input ion nand igon sumer strial lusic, s	com/o y/pro securi	comm. compan duct- ty/bull august	H-QU/ WCN3 06102	
wcn3615										
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables				//ww lcomm. compan duct- ty/bull august -	H-QUA WCN3 06102	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947				com/o y/pro securi	comm. compan duct- ty/bull august	H-QUA WCN3 06102	
	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		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1472		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1473		
wcn3620							
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN3- 061021/1474		
CVSS Scoring Scale							

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1475
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1476
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1477

**2-3 3-4 4-5** 

1-2

0-1

CVSS Scoring Scale

5-6

6-7

8-9

9-10

7-8

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		CVE ID : CVE-2021-30261		
17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN3- 061021/1478
17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1479
17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1480
	17-Sep-21	17-Sep-21 4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon Mobile,	17-Sep-21  18  18  18  18  18  18  18  18  18

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Snapd	ragon W	/earable	S				
			CVE II	D : CVE-	2021-3	0261				
wcn3660b										
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	ointer designation who interest of the contract of the contrac	imprope en the ature toggled uto, ompute, onnectiv onsume ndustria	in vity, r IOT, I IOT,	com/c	comm. ompan duct- ty/bull august	H-QUA WCN3 06102	
Use After Free	17-Sep-21	7.2	kernel becau pointe Comp Conne Indust Mobile Weara Wired	se-after-free vulnerability in ernel graphics driver ecause of storing an invalid pinter in Snapdragon ompute, Snapdragon onnectivity, Snapdragon dustrial IOT, Snapdragon obile, Snapdragon verables, Snapdragon vired Infrastructure and etworking				//ww comm. ompan duct- ty/bull august	H-QUA WCN3 06102	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and			com/c y/prod securit	comm. ompan duct- ty/bull august	H-QUA WCN3 06102		
CVSS Scoring Sca	ile <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID				Pa	tch	NCI	IPC ID
			Netwo	orking						
			CVE II	D : CVE-	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	overflocomm while temple from I Auto, S IOT, S Snapd Snapd Snapd	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261				//ww comm. ompan luct- cy/bull august	H-QUA WCN3 06102	
wcn3680										
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables				//ww comm. ompan luct- cy/bull august	H-QUA WCN3 06102	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired				_	comm. ompan luct- cy/bull august	H-QUA WCN3 06102	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pa	tch	NCI	IPC ID
			Infrast Netwo	ructure rking	and					
			CVE ID	: CVE-2	2021-1	976				
Improper Input Validation	17-Sep-21	7.2	overflocomma while he templated from He Auto, Son IOT, Son Son Son Son Son Son Son Son Son Son Son	ow due to and size nandling te upda (LOS in Sapdrage napdrage ragon Veragon Ve		f input ion n nand igon sumer strial	com/c	comm. ompan duct- ty/bull august	H-QUA WCN3 06102	
			CVE ID	) : CVE-2	2021-3	0261				
wcn3680b										
NULL Pointer Dereference	17-Sep-21	4.9	occurs validat preem enable Snapdi Snapdi Snapdi Snapdi Snapdi	Jull pointer dereference ccurs due to improper alidation when the reemption feature nablement is toggled in napdragon Auto, napdragon Compute, napdragon Connectivity, napdragon Industrial IOT, napdragon Wearables			_	comm. ompan duct- ty/bull august	H-QUA WCN3 06102	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and			_	comm. ompan duct- ty/bull august	H-QUA WCN3 06102		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Networking						
			CVE ID : CVE-	2021-19	947				
Use After Free	17-Sep-21	10	A use after free to improper version device address frame in Snap Snapdragon Consumption of Snapdragon In Snapdragon Version of Snapdragon of Snapdragon version of Snapdragon v	alidations in PD R dragon A ompute, onnective onsumendustrial foice & M Vearable Vired	a of P2P Request Auto, rity, r IOT, IOT, lusic,	•	comm. ompan luct- cy/bull august	H-QUA WCN3 06102	
			CVE ID : CVE-	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	overflow due command size while handling template update from HLOS in Auto, Snapdrag IOT, Snapdrag Snapdragon M Snapdragon V	ossible integer and heap verflow due to lack of input ommand size validation hile handling beacon om HLOS in Snapdragon uto, Snapdragon Consumer OT, Snapdragon Industrial OT, Snapdragon IoT, napdragon Mobile, napdragon Voice & Music, napdragon Wearables			//ww comm. ompan luct- cy/bull august	H-QUA WCN3 06102	
wcn3910									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,			com/c	comm. ompan luct- cy/bull august	H-QUA WCN3 06102	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1493
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN3- 061021/1494
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1495

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID				Pa	tch	NCI	IPC ID
			_	_	oice & M					
			Snapdragon Wearables  CVE ID: CVE-2021-30261							
			CVEII	D : CVE-	2021-3	0261				
wcn3950									T	
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	s due to tion who aption fe ement is aragon C aragon C aragon C aragon In aragon W	eature toggled uto, ompute, onnectiv onsume ndustria Vearable	in vity, r IOT, I IOT, s	com/c	comm. ompan luct- cy/bull august	H-QUA WCN3 06102	
Use After Free	17-Sep-21	7.2	Use-af kernel becau pointe Comp Conne Indust Mobile Weara Wired	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking				//ww comm. ompan duct- cy/bull august	H-QUA WCN3 06102	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired				_	comm. ompan luct- cy/bull august	H-QUA WCN3 06102	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking CVE ID: CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1499
wcn3980					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN3- 061021/1500
wcn3988					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1501
CVSS Scoring Sca	ile <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables		
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1502
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN3- 061021/1503
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1504
CVSS Scoring Sc	ale 0-1	1-2	Auto, Snapdragon Consumer IOT, Snapdragon Industrial	-2021-	8-9 9-

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261		
17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN3- 061021/1505
17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1506
17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1507
	17-Sep-21	17-Sep-21 7.2	Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-30261  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1947  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID : CVE-2021-1939  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon	Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939  17-Sep-21  Vse-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon

Wearables, Snapdragon   Wired Infrastructure and Networking   CVE ID : CVE-2021-1947	Weakness	Publish Date	cvss	Descripti	on & CVE	ID	Pa	tch	NCI	IPC ID
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-30261  Wen3998  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragoust of 1021/15				Wired Infrasti Networking	ructure a	nd				
Improper Input Validation Validation  17-Sep-21  7.2  7.2  7.2  7.2  7.2  7.2  7.3  Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID: CVE-2021-30261  Wcn3998  NULL Pointer Dereference  17-Sep-21  17-Sep-21  17-Sep-21  17-Sep-21  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragons Auto,  Napdragon Wearables to improper validation when the preemption feature enablement is toggled in Snapdragons Auto,  Napdragon Wearables to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,  Napdragon Auto,  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,		17-Sep-21	10	A use after free to improper version of the device address frame in Snap Snapdragon Consumption of Snapdragon of S	w.qual com/c y/prod securit etins/a -2021-	comm. ompan luct- cy/bull nugust	WCN3	-		
NULL Pointer Dereference Dereference  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,  Null pointer dereference w.qualcomm. validation when the preemption feature enablement is toggled in Snapdragon Auto,  Null pointer dereference w.qualcomm. v/product- wCN3- 061021/15	Input Validation	17-Sep-21	7.2	overflow due command size while handlin template upda from HLOS in Auto, Snapdrag IOT, Snapdrag Snapdragon M Snapdragon W Snapdragon W Snapdragon W	w.qual com/c y/prod securit etins/a -2021-	comm. ompan luct- cy/bull nugust	WCN3	-		
NULL Pointer Dereference  NULL Sinapdragon Auto,  NULL Pointer Dereference  Occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,  w.qualcomm. com/compan y/product- security/bull etins/august	wcn3998									
	Pointer Dereference			occurs due to improper validation when the preemption feature enablement is toggled in			w.qual com/c y/prod securit etins/a -2021-	comm. ompan luct- y/bull nugust	WCN3 06102	<b> -</b>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1511
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN3- 061021/1512
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1513

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261		
wcn3999			CVE ID . CVE 2021 30201		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN3- 061021/1514
wcn6740					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN6- 061021/1515
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcomm. com/compan y/product- security/bull	H-QUA- WCN6- 061021/1516

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

CVSS Scoring Scale

	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN6- 061021/1517
wcn6750					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN6- 061021/1518
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,  2-3 3-4 4-5 5-6	https://ww w.qualcomm. com/compan y/product-	H-QUA- WCN6- 061021/1519

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976	security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN6- 061021/1520
wcn6850					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN6- 061021/1521
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid	https://ww w.qualcomm. com/compan	H-QUA- WCN6- 061021/1522
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947	y/product- security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN6- 061021/1523
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WCN6- 061021/1524
wcn6851			N. II	hu. //	H OHA
NULL Pointer	17-Sep-21	4.9	Null pointer dereference occurs due to improper	https://ww w.qualcomm.	H-QUA- WCN6-
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Dereference			validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	com/compan y/product- security/bull etins/august -2021- bulletin	061021/1525
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN6- 061021/1526
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN6- 061021/1527
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://ww w.qualcomm. com/compan	H-QUA- WCN6- 061021/1528
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	y/product- security/bull etins/august -2021- bulletin				
wcn6855								
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN6- 061021/1529			
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA- WCN6- 061021/1530			
wcn6856	wcn6856							
NULL	17-Sep-21	4.9	Null pointer dereference	https://ww	H-QUA-			
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 549 of 861	6-7 7-8	8-9 9-10			

validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID : CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Consumer IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID : CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon ioT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Mobile, Snapdragon Wearables  CVE ID : CVE-2021-30261  whs9410	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
Use After Free  17-Sep-21  10  Improper languate language	Pointer Dereference			validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	com/compan y/product- security/bull etins/august -2021-				
Improper Input Validation Validat	Use After Free	17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	WCN6-			
	Improper Input Validation	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	WCN6-			
CVSS Scoring Scale 0.1 1.2 2.2 2.4 4.5 5.6 6.7 7.0 0.0	whs9410								
		ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10			

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
Improper Input Validation	17-Sep-21	7.2	overfl comm while templ from I Auto, IOT, S IOT, S Snapd Snapd Snapd	ole intego ow due t and size handling ate upda HLOS in S Snapdrag napdrag napdrag ragon W ragon W	to lack of validating beaconstee common section on IoT, lobile, oice & March 1988 March	f input on nand gon sumer strial	com/c y/prod securi	comm. compan duct- ty/bull august	H-QUA WHS9 06102	
wsa8810										
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables				//ww lcomm. compan duct- ty/bull august - n	H-QUA WSA8 06102	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947				com/c y/prod securi	comm. compan duct- ty/bull august	H-QUA WSA8 06102	
Use After	17-Sep-21	10	A use after free can occur due				https:/	//ww	H-QUA	<i>H</i> -
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	WSA8- 061021/1537
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WSA8- 061021/1538
wsa8815					
NULL Pointer Dereference  17-Sep-21 4.9		Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WSA8- 061021/1539	
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WSA8- 061021/1540
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WSA8- 061021/1541
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WSA8- 061021/1542

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

CVSS Scoring Scale

NULL Pointer Dereference  17-Sep-21  Use After Free  17-Sep-21  17-Sep-21  17-Sep-21  17-Sep-21  In the preemption feature enablement is toggled in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Wearables CVE ID: CVE-2021-1939  Use After Free  17-Sep-21  Use After Free  17-Sep-21  In the proper validation when the preemption feature enablement is toggled in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Wearables Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Use After Free  17-Sep-21  In the proper validation when the preemption feature enablement is toggled in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking  Use After Free  17-Sep-21  In the proper validation when the preemption feature enablement is toggled in Snapdragon Connectivity, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  Use After Free  CVE ID: CVE-2021-1976  CVE ID: CVE-2021-1976	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference  17-Sep-21  4.9  4.9  4.9  4.9  4.9  4.9  4.9  4.	wsa8830			L		
Use After Free  17-Sep-21  17-Sep-21  17-Sep-21  18-Sep-21  18-Sep	Pointer	17-Sep-21	4.9	occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	WSA8-
Use After Free  17-Sep-21  10  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Musch w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin		17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	WSA8-
		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	WSA8-

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
Improper Input Validation	17-Sep-21	7.2	overfl comm while templ from I Auto, IOT, S IOT, S Snapd Snapd	ole integonal de la	to lack of validating beacon interest common industrial to the control on IoT, lobile, oice & March 1988 is a solution in IoT,	f input on nand gon sumer strial	com/c y/prod securi	comm. compan duct- ty/bull august	H-QUA WSA8 06102	
wsa8835										
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	ointer designation who intion who intion ferment is dragon Coloragon Coloragon Coloragon Iragon Wiragon Wirago	imprope en the ature toggled uto, ompute, onnectiv onsume ndustrial	in rity, r IOT, IOT, s	com/c y/prod securi	duct- ty/bull august	H-QUA WSA8 06102	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947			com/c y/prod securi	comm. compan duct- ty/bull august	H-QUA WSA8 06102		
Use After	17-Sep-21	10	A use	after fre	e can oc	cur due	https:/	//ww	H-QUA	<i>H</i> -
CVSS Scoring Sca	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	WSA8- 061021/1549
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	H-QUA- WSA8- 061021/1550
Zyxel					
zywall_vpn2s					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Sep-21	5	A directory traversal vulnerability in the web server of the Zyxel VPN2S firmware version 1.12 could allow a remote attacker to gain access to sensitive information.  CVE ID: CVE-2021-35027	https://ww w.zyxel.com/ support/Zyx el_security_a dvisory_for_d irectory_trav ersal_and_co mmand_injec tion_vulnera bilities_of_VP N2S_Firewall	H-ZYX-ZYWA- 061021/1551
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				.shtml	
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	29-Sep-21	7.2	A command injection vulnerability in the CGI program of the Zyxel VPN2S firmware version 1.12 could allow an authenticated, local user to execute arbitrary OS commands.  CVE ID: CVE-2021-35028	https://ww w.zyxel.com/ support/Zyx el_security_a dvisory_for_d irectory_trav ersal_and_co mmand_injec tion_vulnera bilities_of_VP N2S_Firewall .shtml	H-ZYX-ZYWA- 061021/1552
			Operating System		
Apple					
macos	,			,	
Insertion of Sensitive Information into Log File	24-Sep-21	3.6	Tor Browser through 10.5.6 and 11.x through 11.0a4 allows a correlation attack that can compromise the privacy of visits to v2 onion addresses. Exact timestamps of these onion-service visits are logged locally, and an attacker might be able to compare them to timestamp data collected by the destination server (or collected by a rogue site within the Tor network).  CVE ID: CVE-2021-39246	https://gitla b.torproject. org/tpo/core /tor/- /commit/80 c404c4b79f3 bcba3fc4585 d4c62a62a0 4f3ed9, https://gitla b.torproject. org/tpo/core /tor/- /merge_requ ests/434	O-APP-MACO- 061021/1553
Out-of- bounds Read	29-Sep-21	6.8	Adobe InDesign versions 16.3 (and earlier), and 16.3.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	https://help x.adobe.com /security/pr oducts/indes ign/apsb21- 73.html	O-APP-MACO- 061021/1554

p-21 9.3		issue requires user interaction in that a victim must open a malicious TIF file.  CVE ID: CVE-2021-39821  Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary command execution vulnerability. An authenticated attacker could leverage this vulnerability to	https://help x.adobe.com	
p-21 9.3		4.5.11.187646 (and earlier) are affected by an arbitrary command execution vulnerability. An authenticated attacker could	x.adobe.com	
		execute arbitrary commands. User interaction is required to abuse this vulnerability in that a user must open a maliciously crafted .epub file.	/security/pr oducts/Digit al- Editions/aps b21-80.html	O-APP-MACO- 061021/1555
p-21 6.8		Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by an arbitrary file write vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to write an arbitrary file to the system. User interaction is required before product installation to abuse this vulnerability.  CVE ID: CVE-2021-39827	https://help x.adobe.com /security/pr oducts/Digit al- Editions/aps b21-80.html	O-APP-MACO- 061021/1556
p-21 6.8	3	Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by a privilege escalation vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to escalate privileges. User	https://help x.adobe.com /security/pr oducts/Digit al- Editions/aps b21-80.html	O-APP-MACO- 061021/1557
			required before product installation to abuse this vulnerability.  CVE ID: CVE-2021-39827  Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by a privilege escalation vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to	required before product installation to abuse this vulnerability.  CVE ID: CVE-2021-39827  Adobe Digital Editions 4.5.11.187646 (and earlier) are affected by a privilege escalation vulnerability in the Digital Editions installer. An authenticated attacker could leverage this vulnerability to escalate privileges. User  https://help x.adobe.com /security/pr oducts/Digit al-Editions/aps b21-80.html

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
			interaction is required before product installation to abuse this vulnerability.					
			CVE ID : CVE-2021-39828					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Sep-21	9.3	Adobe Photoshop versions 21.2.11 (and earlier) and 22.5 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://help x.adobe.com /security/pr oducts/phot oshop/apsb2 1-84.html	O-APP-MACO- 061021/1558			
			CVE ID : CVE-2021-40709					
Improper Input Validation	29-Sep-21	4.6	Adobe Creative Cloud Desktop Application for macOS version 5.3 (and earlier) is affected by a privilege escalation vulnerability that could allow a normal user to delete the OOBE directory and get permissions of any directory under the administrator authority.  CVE ID: CVE-2021-28547	https://help x.adobe.com /security/pr oducts/creat ive- cloud/apsb2 1-18.html	0-APP-MACO- 061021/1559			
Cisco								
1100-8p_firmware								
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a	https://tools. cisco.com/se curity/center /content/Cis	0-CIS-1100- 061021/1560			
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 559 of 861	6-7 7-8	8-9 9-10			

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	
1120_firmwa	re				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	0-CIS-1120- 061021/1561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1419		
1160_firmwa	re				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	0-CIS-1160- 061021/1562
aironet_1542	a_nrmware			I	
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-AIRO- 061021/1563

**2-3 3-4 4-5** 

1-2

0-1

CVSS Scoring Scale

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419						
aironet_1542i_firmware									
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	O-CIS-AIRO- 061021/1564				
			CVE ID : CVE-2021-1419						
aironet_1562	d_firmware								
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap-	0-CIS-AIRO- 061021/1565				
	ale <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	LLjsGxv	
aironet_1562	e_firmware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-AIRO- 061021/1566
aironet_1562	i_firmware				

**2-3 3-4 4-5** 

1-2

0-1

CVSS Scoring Scale

5-6

7-8

6-7

8-9

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
aironet_1815	m_firmware		configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419		
			A vulnerability in the SSH		
Improper Privilege Management	23-Sep-21	7.2	management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-AIRO- 061021/1569
aironet_1815	t_firmware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	0-CIS-AIRO- 061021/1570
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419		
aironet_1815	w_firmware			l	
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	O-CIS-AIRO- 061021/1571
aironet_1830	e_firmware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points	https://tools. cisco.com/se curity/center	0-CIS-AIRO- 061021/1572

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	/content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	
aironet_1830	i_firmware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-AIRO- 061021/1573

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			equivalent to the root user.		
			CVE ID : CVE-2021-1419		
aironet_1840	i_firmware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-AIRO- 061021/1574
aironet_1850	e_firmware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	0-CIS-AIRO- 061021/1575
CVSS Scoring Sco	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419		
aironet_1850	i_firmware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	O-CIS-AIRO- 061021/1576
aironet_2800	e_firmware		1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco-	O-CIS-AIRO- 061021/1577
CVSS Scoring Sca	le 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	sa-cisco-ap- LLjsGxv	
aironet_2800	i_firmware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-AIRO- 061021/1578

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
aironet_3800	e_firmware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	O-CIS-AIRO- 061021/1579
aironet_3800	i_firmware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	O-CIS-AIRO- 061021/1580

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
aironet_3800	p_firmware		management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419		
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	O-CIS-AIRO- 061021/1581
aironet_4800	_firmware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	0-CIS-AIRO- 061021/1582
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
			improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419					
catalyst_9105	axi_firmwar	e						
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-CATA- 061021/1583			
catalyst_9105	catalyst_9105axw_firmware							
Improper Privilege	23-Sep-21	7.2	A vulnerability in the SSH management feature of	https://tools.cisco.com/se	O-CIS-CATA- 061021/1584			

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Management			multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	
catalyst_9115	axe_firmwar	e			
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-CATA- 061021/1585
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 574 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			the attacker to gain privileges		
			equivalent to the root user.		
. 1 . 044			CVE ID : CVE-2021-1419		
catalyst_9115	axi_firmwar	e			
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	O-CIS-CATA- 061021/1586
catalyst_9117	_firmware			,	
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-CATA- 061021/1587
CVSS Scoring Sco	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419		
catalyst_9120	axe_firmwar	e			
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-CATA- 061021/1588
catalyst_9120	axi_firmwar	е			
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd	0-CIS-CATA- 061021/1589
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 576 of 861	6-7 7-8	8-9 9-10

modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419  A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management Management  23-Sep-21  7.2  A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.				device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.	sa-cisco-ap-	
Improper Privilege Management  A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.	catalyst 9120	axp firmwai	re	CVE ID : CVE-2021-1419		
	Privilege	23-Sep-21	7.2	management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.	cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap-	

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
catalyst_9124	axd_firmwai	re					ı			
Improper Privilege Management	23-Sep-21	7.2	manag multip (APs) local, a modifi- device escala vulner impro opera- manag netwo could vulner affecte manag config success the atte	perability gement fole Cisco platform authenti y files or e and post ted prive rability i per chece tions wit gement i ork admi exploit t rability b ed device gement t guration ssful exp tacker to alent to t D: CVE-	eature of Access	of Points allow a ser to ected in he file SSH A r user sing an h SSH a A d allow ivileges user.	cisco.c curity/ /conte	•		CATA- 1/1591
catalyst_9124	axi_firmwar	e								
Improper Privilege Management	23-Sep-21	7.2	manag multip (APs) local, a modif device escala vulner impro opera manag netwo could vulner	nerability gement f ple Cisco platforn authenti y files or e and pos ted priv per chec tions wit gement i prk admi exploit t rability k ed device	eature of Access I as could cated us the affects illeges. The cate to cking on thin the anistrator his	Points allow a er to ected in he file SSH A r user	cisco.c curity/ /conte	-		CATA- 1/1592
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID						
catalyst_9130	)axe_firmwar	·e	management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419								
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-CATA- 061021/1593						
catalyst_9130	axi_firmwar	e									
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-CATA- 061021/1594						
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 579 of 861	CVSS Scoring Scale							

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			opera manag netwo could vulner affecte manag config succes the atte	per chections with gement in the capility is a deviced and the capility is a deviced and the capility is a capility in the capility is a capility in the capility is a capility in the capility in the capility is a capility in the capility is a capility in the capility in the capility in the capility is a capility in the capility in the capility in the capility is a capility in the	thin the nterface nistrato chis by access through the change. It is gain prother the root	SSH c. A r user sing an ch SSH a A d allow ivileges user.				
catalyst_9800	_firmware									
Improper Privilege Management	23-Sep-21	7.2	managemultipe (APs) local, a modification operate management of the attention of the attention operate management of the attention operate management of the attention operate	gement for platform authenticly files on ted priverability in per check adminations with a device gement to gement t	feature of Access his could cated us in the affects of the tocking on thin the interface his by access to make change. It is on the change of the root the root	of Points allow a ser to ected in he file SSH c. A r user sing an ch SSH a A ld allow ivileges user.	cisco.c	center nt/Cis rityAd /cisco- o-ap-		-CATA- 21/1595
25-3cp-21   7.2						/tools.		-CATA- 21/1596		
Privilege  CVSS Scoring Sca	le <b>0-1</b>	1-2	manag	gement i	4-5	5-6	cisco.c	om/se 7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Management			multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	
catalyst_iw63	00_dcw_firm	ware			
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-CATA- 061021/1597
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 581 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			the attacker to gain privileges equivalent to the root user.		
			CVE ID : CVE-2021-1419		
catalyst_iw63	200 de firmw	aro	CVEID: CVE-2021-1417		
catalyst_lwos	ooo_uc_mmw	are	A ruln anability in the CCII		
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-cisco-ap- LLjsGxv	O-CIS-CATA- 061021/1598
esw-6300_fir	mware				
Improper Privilege Management	23-Sep-21	7.2	A vulnerability in the SSH management feature of multiple Cisco Access Points (APs) platforms could allow a local, authenticated user to modify files on the affected device and possibly gain escalated privileges. The vulnerability is due to improper checking on file operations within the SSH management interface. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-cisco-ap-LLjsGxv	0-CIS-ESW 061021/1599
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			network administrator user could exploit this vulnerability by accessing an affected device through SSH management to make a configuration change. A successful exploit could allow the attacker to gain privileges equivalent to the root user.  CVE ID: CVE-2021-1419					
ios_xe								
Exposure of Resource to Wrong Sphere	23-Sep-21	6.9	A vulnerability in a specific CLI command that is run on Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the configuration database of an affected device. This vulnerability is due to insufficient validation of specific CLI command parameters. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content of the configuration database and gain root-level access to an affected device.  CVE ID: CVE-2021-34723	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa- iosxesdwan- arbfileov- MVOF3ZZn	O-CIS-IOS 061021/1600			
vedge_1000_fi	rmware							
Generation of Error Message Containing Sensitive	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd	O-CIS-VEDG- 061021/1601			
CVSS Scoring Scal	CVSS Scoring Scale							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546	visory/cisco- sa-sd-wan- Fhqh8pKX	
vedge_100b_f	irmware				
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX	O-CIS-VEDG- 061021/1602
vedge_100m_	firmware				
Generation of Error Message Containing	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access	https://tools. cisco.com/se curity/center /content/Cis	0-CIS-VEDG- 061021/1603
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546	coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX	
vedge_100wn	n_firmware				
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-sd-wan-Fhqh8pKX	O-CIS-VEDG- 061021/1604
vedge_100_fir	mware				
Generation of Error Message	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated,	https://tools. cisco.com/se curity/center	0-CIS-VEDG- 061021/1605
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 585 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
Containing Sensitive Information			local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.	/content/Cis coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX			
vedge_2000_f	irmwara		CVE ID : CVE-2021-1546				
veuge_2000_1	II III Wale		A vulnerability in the CLI of				
Generation of Error Message Containing Sensitive Information	23-Sep-21	2.1	Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546	https://tools. cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX	O-CIS-VEDG- 061021/1606		
vedge_5000_firmware							
Generation of Error	23-Sep-21	2.1	A vulnerability in the CLI of Cisco SD-WAN Software	https://tools.cisco.com/se	0-CIS-VEDG- 061021/1607		
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Containing   Sensitive   Sen	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
Generation of Error Message Containing Sensitive Information Information  23-Sep-21  23-Sep-21  23-Sep-21  Containing Sensitive Information  Could allow the attacker to access system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546  Cysum A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546	Containing Sensitive			local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of	/content/Cis coSecurityAd visory/cisco- sa-sd-wan-			
Generation of Error Message Containing Sensitive Information  23-Sep-21  2.1  A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this containing Sensitive Information  23-Sep-21  2.1  A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this consensitive vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.  CVE ID: CVE-2021-1546  Coccom/se curity/center /content/Cis coSecurityAd visory/cisco-sa-sd-wan-Fhqh8pKX  O-CIS-VEDG-061021/1608  visory/cisco-sa-sd-wan-Fhqh8pKX				CVE ID : CVE-2021-1546				
Generation of Error Message Containing Sensitive Information  23-Sep-21  23-Sep-21  23-Sep-21  23-Sep-21  23-Sep-21  23-Sep-21  2.1  Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information. CVE ID: CVE-2021-1546   Cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX  O-CIS-VEDG- 061021/1608	vedge_cloud_f	firmware						
	of Error Message Containing Sensitive Information	•		Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.	cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan-			
Generation 23-Sep-21 2.1 A vulnerability in the CLI of https://tools. O-CIS-VSMA-	vsmart_controller_firmware							
	Generation	23-Sep-21	2.1	A vulnerability in the CLI of	https://tools.	O-CIS-VSMA-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Error Message Containing Sensitive Information			Cisco SD-WAN Software could allow an authenticated, local attacker to access sensitive information. This vulnerability is due to improper protections on file access through the CLI. An attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. A successful exploit could allow the attacker to return portions of an arbitrary file, possibly resulting in the disclosure of sensitive information.	cisco.com/se curity/center /content/Cis coSecurityAd visory/cisco- sa-sd-wan- Fhqh8pKX	061021/1609
			CVE ID : CVE-2021-1546		
D-link					
dcs-5000l_fir	mware				
Improper Authenticati on	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** DCS-5000L v1.05 and DCS-932L v2.17 and older are affecged by Incorrect Acess Control. The use of the basic authentication for the devices command interface allows attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.  CVE ID: CVE-2021-41503	https://ww w.dlink.com/ en/security- bulletin/, https://supp ortannounce ment.us.dlin k.com/annou ncement/pu blication.asp x?name=SAP 10247	0-D-L-DCS 061021/1610
Improper Privilege	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** An Elevated	https://ww w.dlink.com/	0-D-L-DCS 061021/1611
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Management			Privileges issue exists in D-Link DCS-5000L v1.05 and DCS-932L v2.17 and older. The use of the digest-authentication for the devices command interface may allow further attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.  CVE ID: CVE-2021-41504	en/security-bulletin/, https://supp ortannounce ment.us.dlin k.com/annou ncement/pu blication.asp x?name=SAP 10247	
dcs-932l_firm	ıware				
Improper Authenticati on	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** DCS-5000L v1.05 and DCS-932L v2.17 and older are affecged by Incorrect Acess Control. The use of the basic authentication for the devices command interface allows attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.  CVE ID: CVE-2021-41503	https://ww w.dlink.com/ en/security- bulletin/, https://supp ortannounce ment.us.dlin k.com/annou ncement/pu blication.asp x?name=SAP 10247	0-D-L-DCS 061021/1612
Improper Privilege Management	24-Sep-21	5.2	** UNSUPPORTED WHEN ASSIGNED ** An Elevated Privileges issue exists in D- Link DCS-5000L v1.05 and DCS-932L v2.17 and older.	https://ww w.dlink.com/ en/security- bulletin/, https://supp	0-D-L-DCS 061021/1613

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			The use of the digest- authentication for the devices command interface may allow further attack vectors that may compromise the cameras configuration and allow malicious users on the LAN to access the device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.  CVE ID: CVE-2021-41504	ortannounce ment.us.dlin k.com/annou ncement/pu blication.asp x?name=SAP 10247	
Debian					
debian_linux					
Exposure of Sensitive Information to an Unauthorize d Actor	19-Sep-21	5	All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfo from a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.  CVE ID: CVE-2021-40690	https://lists. apache.org/t hread.html/r 8848751b6a 5dd78cc9e9 9d627e74fec faffdfa1bb61 5dce827aad 633%40%3C dev.santuari o.apache.org %3E, https://lists. apache.org/t hread.html/r bdac116aef9 12b563da54 f4c152222c0 754e32fb2f7 85519ac5e0 59f@%3Cco mmits.tomee .apache.org% 3E	O-DEB-DEBI- 061021/1614

6-7

7-8

8-9

9-10

1-2

0-1

Weakness Pu	ıblish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
Improper Privilege 19 Management	9-Sep-21	7.2	loop_rw_iter in fs/io_uring.c in the Linux kernel 5.10 through 5.14.6 allows local users to gain privileges by using IORING_OP_PROVIDE_BUFFE RS to trigger a free of a kernel buffer, as demonstrated by using /proc/ <pid>/maps for exploitation. CVE ID: CVE-2021-41073</pid>	https://git.k ernel.org/pu b/scm/linux /kernel/git/t orvalds/linu x.git/commit /?id=16c8d2 df7ec0eed31 b7d3b61cb1 3206a7fb93 0cc	O-DEB-DEBI- 061021/1615		
Improper Input 16 Validation	6-Sep-21	4.3	Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.  CVE ID: CVE-2021-41079	https://lists. apache.org/t hread.html/r ccdef0349fdf 4fb73a4e440 3095446d7f e6264e0a58 e2df5c67994 34%40%3Ca nnounce.tom cat.apache.or g%3E	O-DEB-DEBI- 061021/1616		
Dlink							
dir-3040_firmwa	are						
Use of Hard- coded 23 Credentials	3-Sep-21	7.5	An information disclosure vulnerability exists in the WiFi Smart Mesh functionality of D-LINK DIR-3040 1.13B03. A specially-crafted network request can lead to command execution. An attacker can connect to the MQTT service to trigger this vulnerability.  CVE ID: CVE-2021-21913	N/A	0-DLI-DIR 061021/1617		
CVE ID : CVE-2021-21913  dir-605l_firmware							

1-2

0-1

5-6

6-7

7-8

8-9

9-10

An informtion disclosure   issue exists in D-LINK-DIR-605 B2 Firmware Version : 2.01MT. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page   CVE ID : CVE-2021-40655	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials  24-Sep-21  4  An information disclosure issue exist in D-LINK-DIR-615 B2 2.01mt. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page CVE ID: CVE-2021-40654  Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing 'externref's from the host to guest Wasm content. To trigger the bug, you have to explicitly pass multiple 'externref's as arguments from host code to a Wasm function, or returning multiple 'externref's to Wasm from a  An information disclosure issue exist in D-LINK-DIR-615 B2 2.01mt. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page CVE ID: CVE-2021-40654  Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing 'externref's from the host to guest Wasm content. To trigger the bug, you have to explicitly pass multiple 'externref's from the host to a Wasm finstance at the same time, either by passing multiple 'externref's as arguments from host code to a Wasm function, or returning multiple 'externref's to Wasm from a	Protected	24-Sep-21	5	issue exists in D-LINK-DIR-605 B2 Firmware Version: 2.01MT. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page	w.dlink.com/ en/security-	
Insufficiently Protected Credentials  24-Sep-21  4	dir-615_firmv	ware				
Use After Free  17-Sep-21  3.3  Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing `externref's from the host to guest Wasm content. To trigger the bug, you have to explicitly pass multiple `externref's from the host to a Wasm instance at the same time, either by passing multiple `externref's as arguments from host code to a Wasm function, or returning multiple `externref's to Wasm from a  Wasmtime is an open source runtime is an open source runtime for WebAssembly & WASI. In Wasmtime from hottose.  Https://github.com/bytec odealliance/wasmtime/s ecurity/advis ories/GHSA-v4cp-h94r-m7xf	Protected	24-Sep-21	4	issue exist in D-LINK-DIR-615 B2 2.01mt. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page	w.dlink.com/ en/security-	
Use After Free  17-Sep-21  3.3  Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing 'externref's from the host to guest Wasm content. To trigger the bug, you have to explicitly pass multiple 'externref's from the host to a Wasm instance at the same time, either by passing multiple 'externref's as arguments from host code to a Wasm function, or returning multiple 'externref's to Wasm from a  Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing 'externref's from the host to dealliance/ wasmtime/s ecurity/advis ories/GHSA-v4cp-h94r-m7xf  0-FED-FEDO-061021/1620	Fedoraprojec	t				
Use After Free  17-Sep-21  3.3  runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing `externref's from the host to guest Wasm content. To trigger the bug, you have to explicitly pass multiple `externref's from the host to a Wasm instance at the same time, either by passing multiple `externref's as arguments from host code to a Wasm function, or returning multiple `externref's to Wasm from a  runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing `externref's from the host odealliance/ wasmtime/s ecurity/advis ories/GHSA-v4cp-h94r-m7xf  0-FED-FEDO-061021/1620	fedora					
		17-Sep-21	3.3	runtime for WebAssembly & WASI. In Wasmtime from version 0.19.0 and before version 0.30.0 there was a use-after-free bug when passing `externref's from the host to guest Wasm content. To trigger the bug, you have to explicitly pass multiple `externref's from the host to a Wasm instance at the same time, either by passing multiple `externref's as arguments from host code to a Wasm function, or returning multiple `externref's to Wasm from a	b.com/bytec odealliance/ wasmtime/s ecurity/advis ories/GHSA- v4cp-h94r-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			defined in the host. If you do		
			not have host code that		
			matches one of these shapes,		
			then you are not impacted. If		
			Wasmtime's		
			`VMExternRefActivationsTabl		
			e` became filled to capacity		
			after passing the first		
			`externref` in, then passing in		
			the second `externref` could		
			trigger a garbage collection.		
			However the first `externref`		
			is not rooted until we pass		
			control to Wasm, and		
			therefore could be reclaimed		
			by the collector if nothing		
			else was holding a reference		
			to it or otherwise keeping it		
			alive. Then, when control was		
			passed to Wasm after the		
			garbage collection, Wasm		
			could use the first `externref`,		
			which at this point has		
			already been freed. We have		
			reason to believe that the		
			effective impact of this bug is		
			relatively small because		
			usage of `externref` is		
			currently quite rare. The bug		
			has been fixed, and users		
			should upgrade to Wasmtime		
			0.30.0. If you cannot upgrade		
			Wasmtime yet, you can avoid		
			the bug by disabling		
			reference types support in		
			Wasmtime by passing `false`		
			to		
			`wasmtime::Config::wasm_ref		
			erence_types`.		
			CVE ID : CVE-2021-39216		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	17-Sep-21	3.3	Wasmtime is an open source runtime for WebAssembly & WASI. In Wasmtime from version 0.26.0 and before version 0.30.0 is affected by a memory unsoundness vulnerability. There was an invalid free and out-of-bounds read and write bug when running Wasm that uses 'externref's in Wasmtime. To trigger this bug, Wasmtime needs to be running Wasm that uses 'externref's, the host creates non-null 'externrefs', Wasmtime performs a garbage collection (GC), and there has to be a Wasm frame on the stack that is at a GC safepoint where there are no live references at this safepoint, and there is a safepoint with live references earlier in this frame's function. Under this scenario, Wasmtime would incorrectly use the GC stack map for the safepoint from earlier in the function instead of the empty safepoint. This would result in Wasmtime treating arbitrary stack slots as 'externref's that needed to be rooted for GC. At the *next* GC, it would be determined that nothing was referencing these bogus 'externref's (because nothing could ever reference them, because they are not really 'externref's)	https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-4873-36h9-wv49,https://github.com/bytecodealliance/wasmtime/commit/398a73f0dd862dbe703212ebae8e34036a18c11c	O-FED-FEDO- 061021/1621

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			and then Wasmtime would deallocate them and run ' <externref as="" drop="">::drop' on them. This results in a free of memory that is not necessarily on the heap (and shouldn't be freed at this moment even if it was), as well as potential out-of-bounds reads and writes. Even though support for 'externref's (via the reference types proposal) is enabled by default, unless you are creating non-null 'externref's in your host code or explicitly triggering GCs, you cannot be affected by this bug. We have reason to believe that the effective impact of this bug is relatively small because usage of 'externref' is currently quite rare. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime at this time, you can avoid this bug by disabling the reference types proposal by passing 'false' to 'wasmtime::Config::wasm_ref erence_types'.  CVE ID: CVE-2021-39218</externref>		
Access of Resource Using Incompatible Type ('Type Confusion')	17-Sep-21	3.3	Wasmtime is an open source runtime for WebAssembly & WASI. Wasmtime before version 0.30.0 is affected by a type confusion vulnerability. As a Rust library the	https://githu b.com/bytec odealliance/ wasmtime/c ommit/b39f 087414f27ae	O-FED-FEDO- 061021/1622

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			`wasmtime` crate clearly	40c44449ed	
			marks which functions are	5d1154e034	
			safe and which are `unsafe`,	49bff,	
			guaranteeing that if	https://githu	
			consumers never use `unsafe`	b.com/bytec	
			then it should not be possible	odealliance/	
			to have memory unsafety	wasmtime/s	
			issues in their embeddings of	ecurity/advis	
			Wasmtime. An issue was	ories/GHSA-	
			discovered in the safe API of	q879-9g95-	
			`Linker::func_*` APIs. These	56mx	
			APIs were previously not		
			sound when one `Engine` was		
			used to create the `Linker`		
			and then a different `Engine`		
			was used to create a `Store`		
			and then the `Linker` was		
			used to instantiate a module		
			into that `Store`. Cross-		
			`Engine` usage of functions is		
			not supported in Wasmtime		
			and this can result in type		
			confusion of function		
			pointers, resulting in being		
			able to safely call a function		
			with the wrong type.		
			Triggering this bug requires		
			using at least two `Engine`		
			values in an embedding and		
			then additionally using two		
			different values with a		
			`Linker` (one at the creation		
			time of the `Linker` and		
			another when instantiating a		
			module with the `Linker`). It's		
			expected that usage of more-		
			than-one `Engine` in an		
			embedding is relatively rare		
			since an `Engine` is intended		
			to be a globally shared		
			resource, so the expectation		

6-7

8-9

7-8

2-3 3-4 4-5

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			is that the impact of this issue is relatively small. The fix implemented is to change this behavior to 'panic!()' in Rust instead of silently allowing it. Using different 'Engine' instances with a 'Linker' is a programmer bug that 'wasmtime' catches at runtime. This bug has been patched and users should upgrade to Wasmtime version 0.30.0. If you cannot upgrade Wasmtime and are using more than one 'Engine' in your embedding it's recommended to instead use only one 'Engine' for the entire program if possible. An 'Engine' is designed to be a globally shared resource that is suitable to have only one for the lifetime of an entire process. If using multiple 'Engine's is required then code should be audited to ensure that 'Linker' is only used with one 'Engine'.  CVE ID: CVE-2021-39219		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-21	7.5	ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.  CVE ID: CVE-2021-39275	https://http d.apache.org /security/vul nerabilities_ 24.html, https://lists. apache.org/t hread.html/r 82c077663f9 759c7df5a66 56f925b3ee4	O-FED-FEDO- 061021/1623

6-7

7-8

8-9

9-10

2-3 3-4 4-5

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
				f55fcd33c88 9ba7cd6870 29@%3Cuse rs.httpd.apac he.org%3E	
Server-Side Request Forgery (SSRF)	16-Sep-21	7.5	A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.  CVE ID: CVE-2021-40438	https://http d.apache.org /security/vul nerabilities_ 24.html, https://lists. apache.org/t hread.html/r 82c077663f9 759c7df5a66 56f925b3ee4 f55fcd33c88 9ba7cd6870 29@%3Cuse rs.httpd.apac he.org%3E	O-FED-FEDO- 061021/1624
Uncontrolled Resource Consumption	20-Sep-21	5	Flask-RESTX (pypi package flask-restx) is a community driven fork of Flask-RESTV before version 0.5.1 is vulnerable to ReDoS (Regular Expression Denial of Service) in email_regex. This is fixed in version 0.5.1.  CVE ID: CVE-2021-32838	https://githu b.com/pytho n- restx/flask- restx/issues/ 372, https://githu b.com/pytho n- restx/flask- restx/commi t/bab31e085 f355dd7385 8fd3715f7ed 71849656da, https://githu b.com/advis ories/GHSA- 3q6g-vf58-	O-FED-FEDO- 061021/1625

CVSS Scoring Scale

5-6

6-7

8-9

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
				7m4g				
NULL Pointer Dereference	16-Sep-21	5	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.  CVE ID: CVE-2021-34798	http://httpd. apache.org/s ecurity/vuln erabilities_2 4.html, https://lists. apache.org/t hread.html/r 82c077663f9 759c7df5a66 56f925b3ee4 f55fcd33c88 9ba7cd6870 29@%3Cuse rs.httpd.apac he.org%3E	0-FED-FED0- 061021/1626			
Out-of- bounds Read	16-Sep-21	5	A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).  CVE ID: CVE-2021-36160	http://httpd. apache.org/s ecurity/vuln erabilities_2 4.html, https://lists. apache.org/t hread.html/r ee7519d714 15ecdd170ff 1889cab552 d71758d2ba 2904a17ded 21a70@%3C cvs.httpd.apa che.org%3E	O-FED-FEDO- 061021/1627			
Google								
android								
Improper Restriction of Operations	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead	https://corp. mediatek.co m/product- security-	0-G00- ANDR- 061021/1628			
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 599 of 861	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			to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05381071.	bulletin/Sept ember-2021	
			CVE ID : CVE-2021-0422		
Missing Initialization of Resource	27-Sep-21	2.1	In memory management driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05385714.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	0-G00- ANDR- 061021/1629
			CVE ID: CVE-2021-0423		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Sep-21	2.1	In memory management driver, there is a possible system crash due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05393787.	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	0-G00- ANDR- 061021/1630
			CVE ID : CVE-2021-0424		
N/A	27-Sep-21	2.1	In memory management driver, there is a possible side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User	https://corp. mediatek.co m/product- security- bulletin/Sept ember-2021	O-GOO- ANDR- 061021/1631
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patcl	h	NCIIPC ID
			interaction is not needed exploitation. Patch ID: ALPS05403499; Issue ID ALPS05400059. CVE ID: CVE-2021-042	:		
Integer Overflow or Wraparound	27-Sep-21	4.6	In memory management driver, there is a possible memory corruption due integer overflow. This collead to local escalation of privilege with no addition execution privileges need User interaction is not needed for exploitation. ID: ALPS05403499; Issue ALPS05411456.  CVE ID: CVE-2021-061	to an buld https://ef mediatel m/produded. security-bulletin/e ID:	k.co uct- - /Sept	-G00- NDR- 61021/1632
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due use after free. This could to local escalation of privation with System execution privileges needed. User interaction is not needed exploitation. Patch ID: ALPS05403499; Issue ID ALPS05425810.  CVE ID: CVE-2021-061	to a lead rilege https://cmediatelm/produsecurity-bulletin/ember-2	k.co uct- - /Sept	-G00- .NDR- 61021/1633
Use After Free	27-Sep-21	4.6	In m4u, there is a possible memory corruption due use after free. This could to local escalation of privileges needed. User interaction is not needed exploitation. Patch ID: ALPS05403499; Issue ID: ALPS05425834.  CVE ID: CVE-2021-061	to a lead vilege https://c mediatel m/produ security- bulletin/ ember-2	k.co uct- - /Sept	-G00- NDR- 61021/1634
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
Out-of- bounds Read	27-Sep-21	4	of bou incorr could disclose execut User in neede ID: AL ALPSO	nds read ect erro lead to i sure wit cion priv nteraction d for exp PS0582'	r handlin nformat h Systen rileges no on is not oloitatio 7145; Iss	ng. This ion n eeded. n. Patch sue ID:	media m/pro securi	duct- ty- n/Sept	0-G00 ANDR 06102	
IBM										
aix										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	Manag vulner site sc vulner embed code in alterir function leadin disclosi session 20840	rable to satisfies ability and arbitra and the Weberler and the incomplete and incomple	I.1.3.10 istored cr This illows us ry JavaS eb UI thu tended	ross- sers to cript is ly sted D:	ange.x bmclo /vulne es/200 https:/ w.ibm uppor	ud.com erabiliti 8405,	O-IBM 06102	-AIX- 1/1636
Allocation of Resources Without Limits or Throttling	16-Sep-21	1.9	Windo Conne 11.5 u condit user to proced the sys memo service 20226	ows (includer versions, condure that stem to a ry.and conduction).	inux, UN ludes Db r) 11.1 a ry specif uld allov unning a t could o run out o ause a d -Force II	o2 and ic v a local cause of enial of D:	uppor s/node 493, https:/ ange.x bmclo	.com/s t/page e/6489 //exch force.i ud.com	0-IBM 06102	-AIX- 1/1637
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204279.  CVE ID: CVE-2021-29810	https://ww w.ibm.com/s upport/page s/node/6491 547, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204279	O-IBM-AIX- 061021/1638
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204330.  CVE ID: CVE-2021-29812	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204330, https://ww w.ibm.com/s upport/page s/node/6491 545	O-IBM-AIX- 061021/1639
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')  CVSS Scoring Sca	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript  2-3 3-4 4-5 5-6	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204331, https://ww w.ibm.com/s upport/page	O-IBM-AIX- 061021/1640 8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204331.	s/node/6491 543	
			CVE ID : CVE-2021-29813		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204334.  CVE ID: CVE-2021-29814	https://ww w.ibm.com/s upport/page s/node/6491 539, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204334	O-IBM-AIX- 061021/1641
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204340.	https://ww w.ibm.com/s upport/page s/node/6491 537, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204340	O-IBM-AIX- 061021/1642

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29815		
Cross-Site Request Forgery (CSRF)	23-Sep-21	4.3	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI 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: 204341.  CVE ID: CVE-2021-29816	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204341, https://ww w.ibm.com/s upport/page s/node/6491 535	O-IBM-AIX- 061021/1643
Exposure of Sensitive Information to an Unauthorize d Actor	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470.  CVE ID: CVE-2021-29825	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204470, https://ww w.ibm.com/s upport/page s/node/6489 499	O-IBM-AIX- 061021/1644
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204824.  CVE ID: CVE-2021-29832	https://ww w.ibm.com/s upport/page s/node/6491 529, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204824	O-IBM-AIX- 061021/1645

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204825.  CVE ID: CVE-2021-29833	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204825, https://ww w.ibm.com/s upport/page s/node/6491 527	O-IBM-AIX- 061021/1646
Cleartext Storage of Sensitive Information	23-Sep-21	2.1	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI displays user credentials in plain clear text which can be read by a local user. IBM X- Force ID: 207610.  CVE ID: CVE-2021-29904	https://ww w.ibm.com/s upport/page s/node/6491 525, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/207610	O-IBM-AIX- 061021/1647
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 207616.	https://ww w.ibm.com/s upport/page s/node/6491 523, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/207616	O-IBM-AIX- 061021/1648
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29905		
powervm_hyp	pervisor				
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	21-Sep-21	4.9	IBM PowerVM Hypervisor FW860, FW930, FW940, and FW950 could allow a local user to create a specially crafted sequence of hypervisor calls from a partition that could crash the system. IBM X-Force ID: 203557.  CVE ID: CVE-2021-29795	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/203557, https://ww w.ibm.com/s upport/page s/node/6490 877	O-IBM- POWE- 061021/1649
kadenvodom	ery				
picoflux_air_f	irmware				
Observable Discrepancy	16-Sep-21	3.3	In Kaden PICOFLUX Air in all known versions an information exposure through observable discrepancy exists. This may give sensitive information (water consumption without distinct values) to third parties.  CVE ID: CVE-2021-34576	https://ww w.fit.vutbr.cz /~polcak/CV E-2021- 34576.en	O-KAD-PICO- 061021/1650
Linux					
linux_kernel					
N/A	20-Sep-21	7.2	arch/mips/net/bpf_jit.c in the Linux kernel through 5.14.6 can generate undesirable machine code when transforming unprivileged cBPF programs, allowing execution of arbitrary code within the kernel context. This occurs because conditional branches can exceed the 128 KB limit	http://www. openwall.co m/lists/oss- security/202 1/09/15/5	O-LIN-LINU- 061021/1651

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			of the MIPS architecture.		
			CVE ID : CVE-2021-38300		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 208405.  CVE ID: CVE-2021-38877	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/208405, https://ww w.ibm.com/s upport/page s/node/6491 521	O-LIN-LINU- 061021/1652
Insertion of Sensitive Information into Log File	24-Sep-21	3.6	Tor Browser through 10.5.6 and 11.x through 11.0a4 allows a correlation attack that can compromise the privacy of visits to v2 onion addresses. Exact timestamps of these onion-service visits are logged locally, and an attacker might be able to compare them to timestamp data collected by the destination server (or collected by a rogue site within the Tor network).  CVE ID: CVE-2021-39246	https://gitla b.torproject. org/tpo/core /tor/- /commit/80 c404c4b79f3 bcba3fc4585 d4c62a62a0 4f3ed9, https://gitla b.torproject. org/tpo/core /tor/- /merge_requ ests/434	0-LIN-LINU- 061021/1653
Improper Privilege Management	19-Sep-21	7.2	loop_rw_iter in fs/io_uring.c in the Linux kernel 5.10 through 5.14.6 allows local users to gain privileges by using IORING_OP_PROVIDE_BUFFE RS to trigger a free of a kernel buffer, as demonstrated by	https://git.k ernel.org/pu b/scm/linux /kernel/git/t orvalds/linu x.git/commit /?id=16c8d2 df7ec0eed31	O-LIN-LINU- 061021/1654

6-7

**2-3 3-4 4-5** 

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			using /proc/ <pid>/maps for exploitation.  CVE ID : CVE-2021-41073</pid>	b7d3b61cb1 3206a7fb93 0cc	
Allocation of Resources Without Limits or Throttling	16-Sep-21	1.9	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267.  CVE ID: CVE-2021-29763	https://ww w.ibm.com/s upport/page s/node/6489 493, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/202267	0-LIN-LINU- 061021/1655
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204279.  CVE ID: CVE-2021-29810	https://ww w.ibm.com/s upport/page s/node/6491 547, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204279	O-LIN-LINU- 061021/1656
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204330, https://ww w.ibm.com/s upport/page	0-LIN-LINU- 061021/1657

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204330.	s/node/6491 545	
			CVE ID : CVE-2021-29812		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204331.	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204331, https://ww w.ibm.com/s upport/page s/node/6491 543	O-LIN-LINU- 061021/1658
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204334.	https://ww w.ibm.com/s upport/page s/node/6491 539, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204334	O-LIN-LINU- 061021/1659

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29814		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204340.  CVE ID: CVE-2021-29815	https://ww w.ibm.com/s upport/page s/node/6491 537, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204340	O-LIN-LINU- 061021/1660
Cross-Site Request Forgery (CSRF)	23-Sep-21	4.3	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI 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: 204341.  CVE ID: CVE-2021-29816	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204341, https://ww w.ibm.com/s upport/page s/node/6491 535	O-LIN-LINU- 061021/1661
Exposure of Sensitive Information to an Unauthorize d Actor	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470.  CVE ID: CVE-2021-29825	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204470, https://ww w.ibm.com/s upport/page s/node/6489 499	O-LIN-LINU- 061021/1662

1-2

0-1

CVSS Scoring Scale

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204824.  CVE ID: CVE-2021-29832	https://ww w.ibm.com/s upport/page s/node/6491 529, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204824	O-LIN-LINU- 061021/1663
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204825.  CVE ID: CVE-2021-29833	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204825, https://ww w.ibm.com/s upport/page s/node/6491 527	O-LIN-LINU- 061021/1664
Cleartext Storage of Sensitive Information  CVSS Scoring Sca	23-Sep-21	2.1	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI displays user credentials in plain clear text which can be read by a local user. IBM X- Force ID: 207610.	https://ww w.ibm.com/s upport/page s/node/6491 525, https://exch ange.xforce.i bmcloud.com	O-LIN-LINU- 061021/1665

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29904	/vulnerabiliti es/207610	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 207616.	https://ww w.ibm.com/s upport/page s/node/6491 523, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/207616	0-LIN-LINU- 061021/1666
			CVE ID : CVE-2021-29905		
Microsoft					
windows			-		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 208405.	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/208405, https://ww w.ibm.com/s upport/page s/node/6491 521	O-MIC-WIND- 061021/1667
			CVE ID : CVE-2021-38877		
Insertion of Sensitive Information into Log File	24-Sep-21	3.6	Tor Browser through 10.5.6 and 11.x through 11.0a4 allows a correlation attack that can compromise the privacy of visits to v2 onion addresses. Exact timestamps	https://gitla b.torproject. org/tpo/core /tor/- /commit/80 c404c4b79f3	O-MIC-WIND- 061021/1668
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

bounds Read  29-Sep-21 6.8 the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious TIF file.  CVE ID : CVE-2021-39821  Adobe Photoshop versions 21.2.11 (and earlier) and 22.5 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  CVE ID : CVE-2021-40709  O61021/1669  O61021/1669  O61021/1669  O61021/1669	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read  29-Sep-21  6.8  Adobe Photoshop versions 21.2.11 (and earlier) and 22.5 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID: CVE-2021-40709  CVE ID: CVE-2021-40709				are logged locally, and an attacker might be able to compare them to timestamp data collected by the destination server (or collected by a rogue site within the Tor network).	d4c62a62a0 4f3ed9, https://gitla b.torproject. org/tpo/core /tor/- /merge_requ	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')  27-Sep-21 Overflow')  27-Sep-21  27-Se		29-Sep-21	6.8	(and earlier), and 16.3.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious TIF file.	x.adobe.com /security/pr oducts/indes ign/apsb21-	0-MIC-WIND- 061021/1669
20 Con 21 4 C	without Checking Size of Input ('Classic Buffer	27-Sep-21	9.3	21.2.11 (and earlier) and 22.5 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted SVG file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	x.adobe.com /security/pr oducts/phot oshop/apsb2	O-MIC-WIND- 061021/1670
Improper 29-Sep-21 4.6 Adobe Creative Cloud https://help O-MIC-WIND-	Improper	29-Sep-21	4.6	Adobe Creative Cloud	https://help	O-MIC-WIND-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Desktop Application for macOS version 5.3 (and earlier) is affected by a privilege escalation vulnerability that could allow a normal user to delete the OOBE directory and get permissions of any directory under the administrator authority.  CVE ID: CVE-2021-28547	x.adobe.com /security/pr oducts/creat ive- cloud/apsb2 1-18.html	061021/1671
Allocation of Resources Without Limits or Throttling	16-Sep-21	1.9	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267.  CVE ID: CVE-2021-29763	https://ww w.ibm.com/s upport/page s/node/6489 493, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/202267	O-MIC-WIND- 061021/1672
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204279.  CVE ID: CVE-2021-29810	https://ww w.ibm.com/s upport/page s/node/6491 547, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204279	O-MIC-WIND- 061021/1673

2-3 3-4 4-5

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204330.  CVE ID: CVE-2021-29812	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204330, https://ww w.ibm.com/s upport/page s/node/6491 545	O-MIC-WIND- 061021/1674
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204331.  CVE ID: CVE-2021-29813	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204331, https://ww w.ibm.com/s upport/page s/node/6491 543	O-MIC-WIND- 061021/1675
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')  CVSS Scoring Sca	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript	https://ww w.ibm.com/s upport/page s/node/6491 539, https://exch ange.xforce.i bmcloud.com	O-MIC-WIND- 061021/1676

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204334.	/vulnerabiliti es/204334	
			CVE ID : CVE-2021-29814		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204340.  CVE ID: CVE-2021-29815	https://ww w.ibm.com/s upport/page s/node/6491 537, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204340	O-MIC-WIND- 061021/1677
Cross-Site Request Forgery (CSRF)	23-Sep-21	4.3	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI 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: 204341.  CVE ID: CVE-2021-29816	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204341, https://ww w.ibm.com/s upport/page s/node/6491 535	O-MIC-WIND- 061021/1678
Exposure of Sensitive Information	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could	https://exch ange.xforce.i bmcloud.com	O-MIC-WIND- 061021/1679

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to an Unauthorize d Actor			disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470.  CVE ID: CVE-2021-29825	/vulnerabiliti es/204470, https://ww w.ibm.com/s upport/page s/node/6489 499	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204824.  CVE ID: CVE-2021-29832	https://ww w.ibm.com/s upport/page s/node/6491 529, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204824	O-MIC-WIND- 061021/1680
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to stored cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 204825.  CVE ID: CVE-2021-29833	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204825, https://ww w.ibm.com/s upport/page s/node/6491 527	O-MIC-WIND- 061021/1681

					NCIIPC ID
Cleartext Storage of Sensitive Information	23-Sep-21	2.1	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI displays user credentials in plain clear text which can be read by a local user. IBM X- Force ID: 207610.  CVE ID: CVE-2021-29904	https://ww w.ibm.com/s upport/page s/node/6491 525, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/207610	O-MIC-WIND- 061021/1682
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-21	3.5	IBM Jazz for Service Management 1.1.3.10 and IBM Tivoli Netcool/OMNIbus_GUI is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 207616.  CVE ID: CVE-2021-29905	https://ww w.ibm.com/s upport/page s/node/6491 523, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/207616	0-MIC-WIND- 061021/1683
Uncontrolled Search Path Element	29-Sep-21	6.9	An uncontrolled search path element privilege escalation vulnerability in Trend Micro HouseCall for Home Networks version 5.3.1225 and below could allow an attacker to escalate privileges by placing a custom crafted file in a specific directory to load a malicious library. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://helpc enter.trendm icro.com/ja- jp/article/T MKA-10621, https://helpc enter.trendm icro.com/en- us/article/t mka-10626	O-MIC-WIND- 061021/1684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2021-32466							
Netgear										
gc108pp_firn	nware									
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 6.0.8.2, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS7510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	O-NET-GC10- 061021/1685					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
gc108p_firmware								
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2, and MS510TXUP before 1.0.4.2.	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	O-NET-GC10- 061021/1686			
	gs108t_firmware							
Improper Authenticati	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n	https://kb.n etgear.com/0	O-NET-GS10-			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			injection in the web UI's	00063978/S	061021/1687
			password field, which - due to	ecurity-	
			several faulty aspects of the	Advisory-for-	
			authentication scheme -	Multiple-	
			allows the attacker to create	Vulnerabiliti	
			(or overwrite) a file with	es-on-Some-	
			specific content (e.g., the "2"	Smart-	
			string). This leads to admin	Switches-	
			session crafting and therefore	PSV-2021-	
			gaining full web UI admin	0140-PSV-	
			privileges by an	2021-0144-	
			unauthenticated attacker.	PSV-2021-	
			This affects GC108P before	0145	
			1.0.8.2, GC108PP before		
			1.0.8.2, GS108Tv3 before		
			7.0.7.2, GS110TPP before		
			7.0.7.2, GS110TPv3 before		
			7.0.7.2, GS110TUP before		
			1.0.5.3, GS308T before		
			1.0.3.2, GS310TP before		
			1.0.3.2, GS710TUP before		
			1.0.5.3, GS716TP before		
			1.0.4.2, GS716TPP before		
			1.0.4.2, GS724TPP before		
			2.0.6.3, GS724TPv2 before		
			2.0.6.3, GS728TPPv2 before		
			6.0.8.2, GS728TPv2 before		
			6.0.8.2, GS750E before		
			1.0.1.10, GS752TPP before		
			6.0.8.2, GS752TPv2 before		
			6.0.8.2, MS510TXM before		
			1.0.4.2, and MS510TXUP		
			before 1.0.4.2.		
			CVE ID : CVE-2021-41314		
gs110tpp_firn	nware				
			Certain NETGEAR smart	https://kb.n	
Improper			switches are affected by a \n	etgear.com/0	
Authenticati	16-Sep-21	8.3	injection in the web UI's	00063978/S	O-NET-GS11-
on	10 JCp 21	0.0	· ·	•	061021/1688
<b>011</b>			password field, which - due to	ecurity-	
			several faulty aspects of the	Advisory-for-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			authentication scheme -	Multiple-		
			allows the attacker to create	Vulnerabiliti		
			(or overwrite) a file with	es-on-Some-		
			specific content (e.g., the "2"	Smart-		
			string). This leads to admin	Switches-		
			session crafting and therefore	PSV-2021-		
			gaining full web UI admin	0140-PSV-		
			privileges by an	2021-0144-		
			unauthenticated attacker.	PSV-2021-		
			This affects GC108P before	0145		
			1.0.8.2, GC108PP before			
			1.0.8.2, GS108Tv3 before			
			7.0.7.2, GS110TPP before			
1			7.0.7.2, GS110TPv3 before			
			7.0.7.2, GS110TUP before			
			1.0.5.3, GS308T before			
			1.0.3.2, GS310TP before			
			1.0.3.2, GS710TUP before			
			1.0.5.3, GS716TP before			
			1.0.4.2, GS716TPP before			
			1.0.4.2, GS724TPP before			
			2.0.6.3, GS724TPv2 before			
			2.0.6.3, GS728TPPv2 before			
			6.0.8.2, GS728TPv2 before			
			6.0.8.2, GS750E before			
			1.0.1.10, GS752TPP before			
			6.0.8.2, GS752TPv2 before			
			6.0.8.2, MS510TXM before			
			1.0.4.2, and MS510TXUP			
			before 1.0.4.2.			
			CVE ID: CVE-2021-41314			
gs110tp_firm	ware					
			Certain NETGEAR smart	https://kb.n		
			switches are affected by a \n	etgear.com/0		
Improper			injection in the web UI's	00063978/S		
Authenticati	16-Sep-21	8.3	password field, which - due to	ecurity-	O-NET-GS11-	
	10-3ch-71	0.5	several faulty aspects of the	Advisory-for-	061021/1689	
on			authentication scheme -	Multiple-		
			allows the attacker to create	Vulnerabiliti		
			(or overwrite) a file with	es-on-Some-		
CVSS Scoring Scale						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPV before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145		
gs110tup_firm	nware					
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021-	O-NET-GS11- 061021/1690	
CVSS Scoring Sca	ile <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10	
CVSS Scoring Scale						

Authenticati on 16-Sep-21 8.3 (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin 5 witches-	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Authenticati on  16-Sep-21  16-Sep-21  18.3  Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin  Certain NETGEAR smart https://kb.n etgear.com/0 00063978/S ecurity-Advisory-for-authentication scheme - Wultiple-Vulnerabiliti es-on-Some-Smart-Smart-Switches-				gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.4.2, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPV2 before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	0140-PSV- 2021-0144- PSV-2021-	
switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" Smart-string). This leads to admin switches are affected by a \n etgear.com/0 00063978/S ecurity-Advisory-for-authentication scheme - Wultiple-Vulnerabilities-on-Some-Some-Some-Some-Some-Some-Some-Some	gs308t_firmw	are				
gaining full web UI admin privileges by an unauthenticated attacker.  PSV-2021-  2021-0144- PSV-2021-	Authenticati	16-Sep-21	8.3	switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an	etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144-	O-NET-GS30- 061021/1691

			This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.4.2, GS716TP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, GS752TPv2 before 6.0.8.2, GS752TPv2 before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314	0145	
Improper Authenticati on	5-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	O-NET-GS31- 061021/1692

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314		
gs710tup_firm	nware		07212		
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	O-NET-GS71- 061021/1693

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

1.0.5.3, GS308T before   1.0.3.2, GS310TP before   1.0.3.2, GS710TUP before   1.0.5.3, GS716TP before   1.0.4.2, GS716TPP before   1.0.4.2, GS724TPPV before   2.0.6.3, GS724TPV2 before   2.0.6.3, GS728TPPV2 before   6.0.8.2, GS750E before   1.0.1.10, GS752TPP before   6.0.8.2, GS750E before   1.0.1.10, GS752TPP before   6.0.8.2, GS752TPV2 before   6.0.8.2, MS510TXM before   1.0.4.2, and MS510TXUP before 1.0.4.2, and MS510TXUP before 1.0.4.2.   CVE ID : CVE-2021-41314   gS716tpp_firmware	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
gs716tpp_firmware    Certain NETGEAR smart   switches are affected by a \n injection in the web UI's   password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GC108PP before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before				1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPv2 before 6.0.8.2, GS728TPv2 before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, GS752TPV2 before 1.0.4.2, and MS510TXUP		
Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before	gs716tnn firi	nware		CVE ID : CVE-2021-41314		
switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before	837 Totpp_III I	IIWaiC		Certain NETCEAR smart		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Authenticati			switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.3.2, GS710TUP before	etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	061021/1694

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314		
gs716tp_firm	ware				
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.4.2, GS716TPP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	O-NET-GS71- 061021/1695

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID: CVE-2021-41314		
gs724tpp_firi	mware				
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before 1.0.3.2, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS716TPP before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPPv2 before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	O-NET-GS72- 061021/1696

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.  CVE ID: CVE-2021-41314		
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart-	O-NET-GS72- 061021/1697
			7.0.7.2, GS110TPP before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before	Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	

**2-3 3-4 4-5** 

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gs728tpp_firr		8.3	6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.  CVE ID: CVE-2021-41314  Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021-	O-NET-GS72- 061021/1698
			7.0.7.2, GS110TUP before	Switches-	

CVE ID : CVE-2021-41314	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.3.2, GS710TUP before 1.0.3.2, GS716TP before 1.0.4.2, GS716TPP before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXMP before 1.0.4.2.				CVE ID : CVE-2021-41314						
switches are affected by a \n injection in the web Ul's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 7.0.7.2, GS110TPP before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPPv2 before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	gs728tp_firm	gs728tp_firmware								
gs750e_firmware	Authenticati	16-Sep-21	8.3	switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS752TPv2 before 6.0.8.2, GS752TPV2 before 6.0.8.2, GS752TPV2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2, and MS510TXUP before 1.0.4.2.	etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021-					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS310TP before 1.0.4.2, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before	https://kb.n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021- 0145	O-NET-GS75- 061021/1700
gs752tpp_firm	nware				
Improper Authenticati on	16-Sep-21	8.3	Certain NETGEAR smart switches are affected by a \n injection in the web UI's	https://kb.n etgear.com/0 00063978/S	O-NET-GS75- 061021/1701
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			password field, which - due to	ecurity-				
			several faulty aspects of the	Advisory-for-				
			authentication scheme -	Multiple-				
			allows the attacker to create	Vulnerabiliti				
			(or overwrite) a file with	es-on-Some-				
			specific content (e.g., the "2"	Smart-				
			string). This leads to admin	Switches-				
			session crafting and therefore	PSV-2021-				
			gaining full web UI admin	0140-PSV-				
			privileges by an	2021-0144-				
			unauthenticated attacker.	PSV-2021-				
			This affects GC108P before	0145				
			1.0.8.2, GC108PP before					
			1.0.8.2, GS108Tv3 before					
			7.0.7.2, GS110TPP before					
			7.0.7.2, GS110TPv3 before					
			7.0.7.2, GS110TUP before					
			1.0.5.3, GS308T before					
			1.0.3.2, GS310TP before					
			1.0.3.2, GS710TUP before					
			1.0.5.3, GS716TP before					
			1.0.4.2, GS716TPP before					
			1.0.4.2, GS724TPP before					
			2.0.6.3, GS724TPv2 before					
			2.0.6.3, GS728TPPv2 before					
			6.0.8.2, GS728TPv2 before					
			6.0.8.2, GS750E before					
			1.0.1.10, GS752TPP before					
			6.0.8.2, GS752TPv2 before					
			6.0.8.2, MS510TXM before					
			1.0.4.2, and MS510TXUP					
			before 1.0.4.2.					
			CVE ID : CVE-2021-41314					
gs752tp_firm	gs752tp_firmware							
			Certain NETGEAR smart	https://kb.n				
I			switches are affected by a \n	etgear.com/0				
Improper	16 0 21	0.2	injection in the web UI's	00063978/S	O-NET-GS75-			
Authenticati	16-Sep-21	8.3	password field, which - due to	ecurity-	061021/1702			
on			several faulty aspects of the	Advisory-for-	•			
			authentication scheme -	Multiple-				
				-				
CVSS Scoring Scale								

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows the attacker to create	Vulnerabiliti	
			(or overwrite) a file with	es-on-Some-	
			specific content (e.g., the "2"	Smart-	
			string). This leads to admin	Switches-	
			session crafting and therefore	PSV-2021-	
			gaining full web UI admin	0140-PSV-	
			privileges by an	2021-0144-	
			unauthenticated attacker.	PSV-2021-	
			This affects GC108P before	0145	
			1.0.8.2, GC108PP before		
			1.0.8.2, GS108Tv3 before		
			7.0.7.2, GS110TPP before		
			7.0.7.2, GS110TPv3 before		
			7.0.7.2, GS110TUP before		
			1.0.5.3, GS308T before		
			1.0.3.2, GS310TP before		
			1.0.3.2, GS710TUP before		
			1.0.5.3, GS716TP before		
			1.0.4.2, GS716TPP before		
			1.0.4.2, GS724TPP before		
			2.0.6.3, GS724TPv2 before		
			2.0.6.3, GS728TPPv2 before		
			6.0.8.2, GS728TPv2 before		
			6.0.8.2, GS750E before		
			1.0.1.10, GS752TPP before		
			6.0.8.2, GS752TPv2 before		
			6.0.8.2, MS510TXM before		
			1.0.4.2, and MS510TXUP		
			before 1.0.4.2.		
			CVE ID : CVE-2021-41314		
ms510txm_fir	rmware				
			Certain NETGEAR smart	https://kb.n	
			switches are affected by a \n	etgear.com/0	
			injection in the web UI's	00063978/S	
Improper			password field, which - due to	ecurity-	
Authenticati	16-Sep-21	8.3	several faulty aspects of the	Advisory-for-	O-NET-MS51-
on	30p <b>-</b> 1		authentication scheme -	Multiple-	061021/1703
- · <del>-</del>			allows the attacker to create	Vulnerabiliti	
				es-on-Some-	
			(or overwrite) a file with	Smart-	
			specific content (e.g., the "2"	Siliai t-	
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 1.0.5.3, GS308T before 1.0.5.3, GS308T before 1.0.5.3, GS310TP before 1.0.5.3, GS310TP before 1.0.5.3, GS710TUP before 1.0.5.3, GS716TPP before 1.0.4.2, GS716TPP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPv2 before 6.0.8.2, GS752TPv2 before 6.0.8.2, GS752TPv before 6.0.8.2, GS752TPv before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, GS752TPv2 before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2. CVE ID : CVE-2021-41314	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
ns510txup_firmware				string). This leads to admin session crafting and therefore gaining full web UI admin privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.3.2, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPV2 before 2.0.6.3, GS724TPV2 before 2.0.6.3, GS728TPV2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP	Switches- PSV-2021- 0140-PSV- 2021-0144- PSV-2021-	
Certain NETGEAR smart https://kh.n	ms510txup_f	irmware				
switches are affected by a \n injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create vulnerability of 100063978/S ecurity-  8.3  8.4  Switches are affected by a \n etgear.com/0 00063978/S ecurity- Advisory-for- Multiple- Vulnerability 061021/1704	Improper Authenticati on	16-Sep-21	8.3	injection in the web UI's password field, which - due to several faulty aspects of the authentication scheme - allows the attacker to create (or overwrite) a file with specific content (e.g., the "2" string). This leads to admin session crafting and therefore	00063978/S ecurity- Advisory-for- Multiple- Vulnerabiliti es-on-Some- Smart- Switches- PSV-2021-	
CVSS Scoring Scale	CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges by an unauthenticated attacker. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TPV3 before 7.0.7.2, GS110TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.4.2, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPv2 before 6.0.8.2, GS750E before 1.0.1.10, GS752TPP before 6.0.8.2, GS752TPV2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.  CVE ID: CVE-2021-41314	2021-0144- PSV-2021- 0145	
r6020_firmwa	ire				
Improper Neutralizatio n of Special Elements used in a Command ('Command Injection')	17-Sep-21	9	setup.cgi on NETGEAR R6020 1.0.0.48 devices allows an admin to execute arbitrary shell commands via shell metacharacters in the ntp_server field.  CVE ID: CVE-2021-41383	N/A	O-NET-R602- 061021/1705
opengroup					
unix					
Allocation of Resources Without Limits or	16-Sep-21	1.9	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific	https://ww w.ibm.com/s upport/page s/node/6489	O-OPE-UNIX- 061021/1706
CVSS Scoring Scal	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Throttling			conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267.  CVE ID: CVE-2021-29763	493, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/202267	
Exposure of Sensitive Information to an Unauthorize d Actor	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470.  CVE ID: CVE-2021-29825	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204470, https://ww w.ibm.com/s upport/page s/node/6489 499	O-OPE-UNIX- 061021/1707
Oracle					
linux					
N/A	24-Sep-21	7.2	Vulnerability in Oracle Linux (component: OSwatcher). Supported versions that are affected are 7 and 8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Linux executes to compromise Oracle Linux. Successful attacks of this vulnerability can result in takeover of Oracle Linux. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/U I:N/S:U/C:H/I:H/A:H).	https://linux .oracle.com/ errata/ELSA- 2021- 9444.html	0-0RA-LINU- 061021/1708
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2021-2464			
solaris						
Allocation of Resources Without Limits or Throttling	16-Sep-21	1.9	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 under very specific conditions, could allow a local user to keep running a procedure that could cause the system to run out of memory.and cause a denial of service. IBM X-Force ID: 202267.  CVE ID: CVE-2021-29763	https://ww w.ibm.com/s upport/page s/node/6489 493, https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/202267	O-ORA-SOLA- 061021/1709 O-ORA-SOLA- 061021/1710	
Exposure of Sensitive Information to an Unauthorize d Actor	16-Sep-21	5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP. IBM X-Force ID: 204470.  CVE ID: CVE-2021-29825	https://exch ange.xforce.i bmcloud.com /vulnerabiliti es/204470, https://ww w.ibm.com/s upport/page s/node/6489 499		
Phoenixconta	ct					
axc_f_1152_fii	rmware					
Improper Input Validation	27-Sep-21 7.8		Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID: CVE-2021-34570	https://cert. vde.com/en/ advisories/V DE-2021- 029/	O-PHO-AXC 061021/1711	
axc_f_2152_fii	rmware					
Improper Input Validation	27-Sep-21	7.8	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack	https://cert. vde.com/en/ advisories/V DE-2021-	O-PHO-AXC 061021/1712	
CVSS Scoring Sca	le 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10	

through special crafted JSON requests.  CVE ID : CVE-2021-34570    Axc.f. 2152_starterkit_firmware	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
Axc_f_2152_starterkit_fir=ware  Improper Input Validation  Z7-Sep-21 7.8					029/		
Improper Input Validation 27-Sep-21 7.8   Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests. CVE ID : CVE-2021-34570   CVE ID : C				•			
Improper Input Validation 27-Sep-21 7.8   Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID : CVE-2021-34570   CO-PHO-AXC-061021/1713   CO-PHO-AXC-061021/1713   CO-PHO-AXC-061021/1713   CO-PHO-AXC-061021/1713   CO-PHO-AXC-061021/1713   CO-PHO-AXC-061021/1713   CO-PHO-AXC-061021/1713   CO-PHO-AXC-061021/1713   CO-PHO-AXC-061021/1713   CO-PHO-AXC-061021/1714   CO-PHO-PLCN-061021/1715   CO-PHO-PLCN-061021/1716   CO-PHO-PL	ava f 2152 st	autaultit fium		CVE ID: CVE-2021-34570			
Improper Input Validation 27-Sep-21 7.8   PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID : CVE-2021-34570   CPHO-AXC_061021/1713   CPHO-AXC_061021/1714   CPHO-AXC_061021/1715   CPHO-AXC_061021/1715   CPHO-AXC_061021/1715   CPHO-AXC_061021/1715   CPHO-AXC_061021/1715   CPHO-AXC_061021/1716   CPHO-AXC_06102	axc_i_2152_st	arterkit_iirii	iware	M let l Dl		l	
Improper   27-Sep-21   7.8   Multiple Phoenix Contact   PLCnext control devices in versions prior to 2021.0.5   LTS are prone to a DoS attack through special crafted JSON requests.   CVE ID : CVE-2021-34570   CPHO-AXC061021/1714	Input	27-Sep-21	7.8	PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.	vde.com/en/ advisories/V DE-2021-	_	
Improper Input Validation	axc_f_3152_fi	rmware					
Improper Input Validation 27-Sep-21 7.8 Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID: CVE-2021-34570 DE-2021-029/  Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 DE-2021-029/  Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  Validation 27-Sep-21 7.8 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID: CVE-2021-34570 DE-2021-029/  CVE ID: CVE-2021-34570	Input	27-Sep-21	7.8	PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.	vde.com/en/ advisories/V DE-2021-	_	
Improper Input Validation 27-Sep-21 7.8 Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID: CVE-2021-34570 DE-2021-029/  Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 DE-2021-029/  Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  Validation 27-Sep-21 7.8 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID: CVE-2021-34570 DE-2021-029/  CVE ID: CVE-2021-34570	plcnext techn	l ology starte	rkit fir	mware			
Improper Input Validation 27-Sep-21 7.8 Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID: CVE-2021-34570 https://cert. vde.com/en/advisories/V DE-2021-029/	Improper Input	Multiple Phoenix Contact PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  Multiple Phoenix Contact https://cert. vde.com/en/ advisories/V DE-2021- 029/					
Improper Input Validation 27-Sep-21 7.8 PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.  CVE ID : CVE-2021-34570 https://cert. vde.com/en/ advisories/V DE-2021-029/	rfc_4072s_firm	mware					
Qualcomm	Input	27-Sep-21	7.8	PLCnext control devices in versions prior to 2021.0.5 LTS are prone to a DoS attack through special crafted JSON requests.	vde.com/en/ advisories/V DE-2021-	_	
	Qualcomm						

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Free  Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, O-QUA-APQ8-	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
NULL Pointer Dereference 17-Sep-21 Use After Free 17-Sep-21 17-Sep-21 18-Sep-21 18-Sep-21 18-Sep-21 18-Sep-21 19-Sep-21 19-Sep	apq8009w_fin	mware						
Use After Free   17-Sep-21   10	Pointer	17-Sep-21	4.9	occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	ccurs due to improper alidation when the reemption feature nablement is toggled in napdragon Auto, napdragon Compute, napdragon Connectivity, napdragon Industrial IOT, napdragon Wearables  VE ID : CVE-2021-1939  https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin			
Use After Free  17-Sep-21  Use After Free  10  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, https://www.qualcomm.com/compan y/product-security/bull etins/august -2021-bulletin		17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	O-QUA-APQ8- 061021/1718		
CVE ID : CVE-2021-1976		17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	0-QUA-APQ8- 061021/1719		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Auto, Shapuragon Consumer   5,7		0-QUA-APQ8- 061021/1720
apq8009_firm	ıware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939		O-QUA-APQ8- 061021/1721
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-APQ8- 061021/1722

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		CVE ID : CVE-2021-1976		
17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-APQ8- 061021/1723
nware		CV21D 1 CV2 2021 00201		
ii wai c		Null pointer dereference		
17-Sep-21	4.9	occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-APQ8- 061021/1724
17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-APQ8- 061021/1725
	17-Sep-21 17-Sep-21	17-Sep-21 7.2 17-Sep-21 4.9	CVE ID : CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon  Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID : CVE-2021-30261  Numare  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID : CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Connectivity, Snapdragon Compute, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired	17-Sep-21  18  18  18  18  18  18  18  18  18

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID: CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-APQ8- 061021/1726
apq8037_firm	iware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8- 061021/1727
apq8053_firm	iware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-APQ8- 061021/1728
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-APQ8- 061021/1729
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-APQ8- 061021/1730
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-APQ8- 061021/1731
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 646 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	ption & CVE ID Patch				
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables					
			CVE ID: CVE-2021-30261					
apq8064au_firmware								
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-APQ8- 061021/1732			
apq8084_firm	iware							
Improper Input Validation  17-Sep-21 7.2		7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-APQ8- 061021/1733			
			CVE ID : CVE-2021-30261					
apq8096au_fi	rmware		A use after free can easur due	https://www				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	0-QUA-APQ8- 061021/1734			
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10			

Weakness	Publish Date	cvss	D	escriptio	n & CVE	ID	Pat	ch	NCI	IPC ID
			Snapdr Snapdr Snapdr Snapdr Snapdr Snapdr Infrast	ragon Coragon Coragon Intragon Woragon Woragon Woructure  rking  C: CVE-2	onnective onsume dustria oice & M Gearable Gired and	vity, r IOT, I IOT, Iusic, es,	securit etins/a -2021- bulletin	ugust		
Improper Input Validation	17-Sep-21	7.2	Possible overflood command while he template from He Auto, Stranger Snaper Snaper Snaper CVE ID	f input ion n nand igon sumer strial	https:/ w.qual- com/co y/prod securit etins/a -2021- bulletin	comm. compan luct- y/bull lugust	_	A-APQ8- 21/1735		
aqt1000_firm	ware									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939				https:/ w.qual- com/cd y/prod securit etins/a -2021- bulletin	comm. compan luct- y/bull lugust	_	A-AQT1- 21/1736
Use After Free	17-Sep-21	10	to imp	roper va	alidation	cur due n of P2P Request	https:/ w.qual com/co	comm.	_	A-AQT1- 21/1737
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	y/product- security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-AQT1- 061021/1738
ar6003_firmw	vare				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-AR60- 061021/1739
ar7420_firmw	vare				
CVSS Scoring Sca	ile <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-AR74- 061021/1740
ar8031_firmv	vare				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-AR80- 061021/1741
ar8035_firmv	vare				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-AR80- 061021/1742
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
ar9380_firmv	varo		CVE ID : CVE-2021-1976		
al 9300_III III v	vare		Use-after-free vulnerability in		
Use After Free	17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-AR93- 061021/1743
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-AR93- 061021/1744
csr6030_firm	ware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://ww w.qualcomm. com/compan y/product- security/bull	0-QUA-CSR6- 061021/1745
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 651 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	etins/august -2021- bulletin	
csr8811_firm	ware		CVE ID : CVE-2021-30201		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSR8- 061021/1746
csra6620_firm	nware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-CSRA- 061021/1747

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
csra6640_firn	nware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-CSRA- 061021/1748
104004 6			CVE ID : CVE-2021-1976		
csrb31024_fin	mware			,	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-CSRB- 061021/1749
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-CSRB- 061021/1750
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID Patch		NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
fsm10055_fir	mware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-FSM1- 061021/1751
fsm10056_fir	mware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-FSM1- 061021/1752
ipq4018_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://ww w.qualcomm. com/compan	0-QUA-IPQ4- 061021/1753
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	y/product- security/bull etins/august -2021- bulletin	
ipq4019_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ4- 061021/1754
ipq4028_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-IPQ4- 061021/1755
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Description & CVE ID Patch	
			Networking		
			CVE ID : CVE-2021-1976		
ipq4029_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-IPQ4- 061021/1756
ipq5010_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-IPQ5- 061021/1757
ipq5018_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcomm. com/compan y/product- security/bull	O-QUA-IPQ5- 061021/1758
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 <b>9-10</b>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976	etins/august -2021- bulletin	
ipq5028_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ5- 061021/1759
ipq6000_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-IPQ6- 061021/1760
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	<b>Publish Date</b>	CVSS	Descrip	tion & CVE	ID	Pa	tch	NCI	IPC ID
ipq6005_firm	ware								
Use After Free	17-Sep-21	10	A use after for to improper device address frame in Sna Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Infrastructure Networking CVE ID: CVI	com/c	comm. ompan luct- cy/bull nugust	_	A-IPQ6- 21/1761		
ipq6010_firm	ware								
Use After Free	17-Sep-21	10	to improper device addre frame in Sna Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Infrastructu	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking				_	A-IPQ6- 21/1762
ipq6018_firm	ware								
Use After Free	17-Sep-21	10	tr/product			A-IPQ6- 21/1763			
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976	bulletin	
ipq6028_firn	nware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-IPQ6- 061021/1764
ipq8064_firn	nware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8- 061021/1765
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	O-QUA-IPQ8- 061021/1766

2-3 3-4 4-5

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	security/bull etins/august -2021- bulletin	
			CVE ID : CVE-2021-1976		
ipq8065_firm	ware			T	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-IPQ8- 061021/1767
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-IPQ8- 061021/1768
ipq8068_firm	ware				

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-IPQ8- 061021/1769
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8- 061021/1770
ipq8069_firm	ware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8- 061021/1771
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-IPQ8- 061021/1772
ipq8070a_firm	nware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-IPQ8- 061021/1773
ipq8070_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-IPQ8- 061021/1774
CVSS Scoring Sca	ile 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			
			CVE ID: CVE-2021-1976			
ipq8071a_firi	nware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8- 061021/1775	
ipq8071_firm	ware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-IPQ8- 061021/1776	
ipq8072a_firmware						
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P	https://ww w.qualcomm.	O-QUA-IPQ8- 061021/1777	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	com/compan y/product- security/bull etins/august -2021- bulletin	
ipq8072_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-IPQ8- 061021/1778
ipq8074a_firi	nware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8- 061021/1779
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Infrastructure and				
			Networking				
			CVE ID : CVE-2021-1976				
ipq8074_firm	ware			T			
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8- 061021/1780		
			CVE ID: CVE-2021-1976				
ipq8076a_firr	nware						
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8- 061021/1781		
ipq8076_firmware							
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	O-QUA-IPQ8- 061021/1782		
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2021-1976			
ipq8173_firm	ware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-IPQ8- 061021/1785	
ipq8174_firm	ware					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-IPQ8- 061021/1786	
mdm8207_firmware						
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	O-QUA- MDM8- 061021/1787	
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 667 of 861	6-7 7-8	8-9 9-10	

IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261   Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Input  17-Sep-21  7.2  Auto, Snapdragon IoT, Snapdragon IoT, Snapdragon Husic, Snapdragon Wearables  -2021- bulletin  https://ww w.qualcomm. com/compan y/product- security/bull MDM8-	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
Improper Input Validation Input V				IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,					
Improper Input Validation Input Valid				CVE ID : CVE-2021-30261					
Improper Input Validation Input Va	mdm8215m_f	mdm8215m_firmware							
Improper Input Validation Validat	Input	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	=			
Improper Input Validation Validation Improper Input Validation Validation  Improper Input Validation  Imposer Input Validation  Validation  Improper Input Validation  Imposer Input Validation	mdm8215_fir	mware							
Improper 17-Sep-21 7.2 Possible integer and heap https://ww 0-QUA-	Improper Input Validation	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	=			
1/-3CD-21   /.2	mdm8615m_firmware								
		17-Sep-21	7.2	_		_			

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	com/compan y/product- security/bull etins/august -2021- bulletin	061021/1790
mdm9150_fir	mware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MDM9- 061021/1791
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MDM9- 061021/1792
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Snapdragon Voice & Music,			
			Snapdragon Wearables			
			CVE ID : CVE-2021-30261			
mdm9207_fir	mware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MDM9- 061021/1796	
mdm9215_fir	mware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MDM9- 061021/1797	
mdm9230_firmware						
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	O-QUA- MDM9- 061021/1798	
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID				
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	-2021- bulletin					
1 0070 8			CVE ID : CVE-2021-30261						
mdm9250_fir	mdm9250_firmware								
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MDM9- 061021/1799				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MDM9- 061021/1800				
mdm9310_firmware									
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://ww w.qualcomm.	O-QUA- MDM9-				
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 672 of 861	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Descr	iption & CVE	ID	Pa	tch	NCI	IPC ID
			CVE ID : C	VE-2021-1	976				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			com/c	comm. ompan luct- cy/bull august	0-QUA MDM9 06102	
	S www.vo.wo		CVE ID : C	VE-2U21-3	0201				
mdm9615m_t	mmware		D 411						
Improper Input Validation	17-Sep-21	7.2	overflow d command s while hand template u from HLOS Auto, Snap IOT, Snapd IOT, Snapd Snapdrago Snapdrago	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables			//ww comm. ompan luct- cy/bull august	0-QUA MDM9 06102	
mdm9615_fir	mware								
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,			_	comm. ompan luct- cy/bull august	O-QUA MDM9 06102	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-	4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
mdm9625_fir	muara		CVE ID : CVE-2021-30201		
11101119025_111	iliwale		Descible integer and been	<u> </u>	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- MDM9- 061021/1807
			CVE ID : CVE-2021-30261		
mdm9626_fir	mware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- MDM9- 061021/1808
mdm9628_fir	mware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcomm. com/compan y/product- security/bull	O-QUA- MDM9- 061021/1809
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	etins/august -2021- bulletin		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MDM9- 061021/1810	
mdm9630_fir	mware					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA- MDM9- 061021/1811	
mdm9635m_firmware						
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 676 of 861	6-7 7-8	8-9 9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	MDM9- 061021/1812
mdm9640_fir	rmware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- MDM9- 061021/1813
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MDM9- 061021/1814

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

CVSS Scoring Scale

Weakness	Publish Date	CVSS		escriptio	on & CVE	ID	Pa	tch	NCI	IPC ID
			CVE ID	) : CVE-2	2021-30	0261				
mdm9645_fir	mware									
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			com/c	comm. ompan duct- ty/bull august	0-QUA MDM9 06102		
mdm9650_fir	mware									
Use After Free	17-Sep-21	10	to impledevice frame in Snapdi Snapdi Snapdi Snapdi Snapdi Snapdi Infrast Netwo	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		com/c	comm. ompan duct- ty/bull august	0-QUA MDM9 06102		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,			com/c	comm. ompan duct- ty/bull august	0-QUA MDM9 06102		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
mdm9655_fir	mware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA- MDM9- 061021/1818
			CVE ID : CVE-2021-30261		
msm8108_fir	mware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MSM8- 061021/1819
msm8208_fir	mware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://ww w.qualcomm. com/compan y/product- security/bull	O-QUA- MSM8- 061021/1820
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			from HLOS in Auto, Snapdrag IOT, Snapdrag IOT, Snapdrag Snapdragon W Snapdragon W Snapdragon W	ngon Con gon Indus gon IoT, Mobile, Yoice & M Vearable	sumer strial usic,	etins/a -2021- bulleti			
msm8209_fir	mware								
Improper Input Validation	17-Sep-21	7.2	Possible integ overflow due command size while handling template update from HLOS in Auto, Snapdrag IOT, Snapdrag IOT, Snapdrag Snapdragon M Snapdragon V Snapdragon V	to lack of e validati g beacon ate comn Snapdra gon Con gon Indus gon IoT, Tobile, Voice & M	f input on hand gon sumer strial fusic,	com/c	comm. ompan luct- cy/bull august	0-QU/ MSM8 06102	
msm8608_fir	mware								
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261		com/c	comm. ompan luct- cy/bull august	0-QUA MSM8 06102		
msm8909w_f	firmware								
NULL	17-Sep-21	4.9	Null pointer d	ereferen	ce	https:/	//ww	O-QUA	۱-
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	MSM8- 061021/1823
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MSM8- 061021/1824
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- MSM8- 061021/1825
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://ww w.qualcomm.	O-QUA- MSM8-
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 681 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	com/compan y/product- security/bull etins/august -2021- bulletin	061021/1826
msm8917_fir	mware			T	
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MSM8- 061021/1827
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MSM8- 061021/1828
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	MSM8- 061021/1829
msm8920_fir	mware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- MSM8- 061021/1830
msm8937_fir	mware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- MSM8- 061021/1831
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
msm8940_fir	mware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MSM8- 061021/1832
msm8953_fir	mware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MSM8- 061021/1833
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MSM8- 061021/1834

Weakness	Publish Date	CVSS	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Networking						
			CVE ID : CVE-2	2021-19	947				
Use After Free	17-Sep-21	10	to improper value device address frame in Snaper Sn	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976				0-QU/ MSM8 06102	
			CVE ID : CVE-2	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	Possible integers overflow due to command size while handling template update from HLOS in State of the state	com/c	comm. ompan luct- cy/bull august	0-QU/ MSM8 06102			
msm8976sg_f	firmware								
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,				comm. ompan luct- cy/bull august	0-QU <i>F</i> MSM8 06102	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261		
msm8976_fir	mware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MSM8- 061021/1838
msm8996au_	<u>firmware</u>				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- MSM8- 061021/1839
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://ww w.qualcomm. com/compan y/product- security/bull	O-QUA- MSM8- 061021/1840

6-7

**2-3 3-4 4-5** 

8-9

9-10

7-8

CVSS Scoring Scale

Weakness F	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	etins/august -2021- bulletin	
pmp8074_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-PMP8- 061021/1841
qca1990_firmw	vare				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA1- 061021/1842
qca4004_firmw	vare				

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA4- 061021/1843
qca4020_firm	ware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA4- 061021/1844
qca4024_firm	ware			l	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA4- 061021/1845
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	I	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Netwo	rking						
			CVE II	O: CVE-	2021-1	976				
qca6174a_firi	mware									
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939				//ww comm. ompan duct- cy/bull august	_	A-QCA6- 21/1846
Use After Free	17-Sep-21	10	to imp device frame Snapd Snapd Snapd Snapd Snapd Snapd Infrast	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking				//ww comm. ompan duct- cy/bull august	_	A-QCA6- 21/1847
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,			_	comm. ompan luct- cy/bull august	_	A-QCA6- 21/1848	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			Snapdragon Voice & Music,								
			Snapdragon Wearables								
			CVE ID : CVE-2021-30261								
qca6174_firm	qca6174_firmware										
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1849						
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA6- 061021/1850						
qca6310_firm	ware										
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	0-QUA-QCA6- 061021/1851						
CVSS Scoring Sca	ile 0-1	1-2	2-3 3-4 4-5 5-6 Page 690 of 861	6-7 7-8	8-9 9-10						

Weakness	Publish Date	cvss	Descri	otion & CVE	ID	Pat	tch	NCI	IPC ID
			Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor	Connective Consumer Industrial Wearable	rity, r IOT, IOT, s	-2021- bulleti			
Use After Free	17-Sep-21	10	A use after to improper device addr frame in Sn Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Infrastructu Networking CVE ID : CV	https:/ w.qual com/co y/prod securit etins/a -2021- bulleti	comm. compan luct- y/bull nugust	_	A-QCA6- 21/1852		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			https:/ w.qual com/co y/prod securit etins/a -2021- bulletin	comm. compan luct- y/bull nugust		A-QCA6- 21/1853
qca6320_firm	ware								
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon			https:/ w.qual com/co y/prod securit	comm. ompan luct-	_	A-QCA6- 21/1854
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pa	tch	NCI	IPC ID
			Industr Mobile Wearal Wired Netwo	rial IOT, , Snapd bles, Sna Infrastr rking	Snapdra , Snapdr ragon apdrago ucture a	ragon on and	etins/a -2021- bulleti			
Use After Free	17-Sep-21	10	to improduce frame in Snapdir	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976				/ww comm. ompan luct- cy/bull nugust	_	A-QCA6- 21/1855
Improper Input Validation	17-Sep-21	7.2	overflocomma while he templa from He Auto, Son IOT, Son Son Son Son Son Son Son Son Son Son	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261		•	comm. compan luct- cy/bull nugust	_	A-QCA6- 21/1856	
qca6335_firm	iware									
NULL Pointer Dereference	17-Sep-21	4.9	occurs validat	Null pointer dereference occurs due to improper validation when the preemption feature				/ww comm. ompan luct-	_	A-QCA6- 21/1857
CVSS Scoring Sca	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Desc	cription	& CVE	ID	Pa	tch	NCI	PC ID
			Snapdrage Snapdrage Snapdrage Snapdrage Snapdrage Snapdrage	enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939				y/bull nugust n		
Use After Free	17-Sep-21	10	A use afte to improp device add frame in S Snapdrage Snapdrage Snapdrage Snapdrage Snapdrage Snapdrage Infrastruct Networkin CVE ID: C	dress is Snapdress is con Con Con Con Con Con Weston Windows is con Windows in the Windows is con Windows is con Windows in the Windows in th	idatior in PD F ragon A mpute, nnectiv nsume lustrial ice & M earable red ind	a of P2P Request Auto, rity, r IOT, IOT, lusic, s,	_	comm. compan luct- cy/bull nugust	_	-QCA6- 1/1858
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261		_	comm. ompan luct- y/bull nugust	_	-QCA6- 1/1859		
qca6390_firm	iware									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the				_	/ww comm. ompan	_	-QCA6- 1/1860
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	y/product- security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1861
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1862
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://ww w.qualcomm. com/compan y/product-	0-QUA-QCA6- 061021/1863

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	security/bull etins/august -2021- bulletin	
qca6391_firm	ware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1864
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1865
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcomm. com/compan y/product- security/bull	0-QUA-QCA6- 061021/1866

			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-QCA6- 061021/1867
qca6420_firm	ware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1868
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	0-QUA-QCA6- 061021/1869

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976	security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1870
qca6421_firm	ıware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1871
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://ww w.qualcomm. com/compan	0-QUA-QCA6- 061021/1872
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID					
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	y/product- security/bull etins/august -2021- bulletin						
qca6426_firm	qca6426_firmware									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1873					
Use After Free  17-Sep-21  7.2  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon com/compan Compute, Snapdragon y/product-security/bull etins/august verables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947    Use-after-free vulnerability in kernel graphics driver because of storing an invalid https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2-2021-bulletin										
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,  2-3 3-4 4-5 5-6	https://ww w.qualcomm. com/compan y/product-	0-QUA-QCA6- 061021/1875					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976									
Improper Input Validation Validation  Improper Input Validation Validation  Improper Input Validation  Validation  Validation  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables CVE ID: CVE-2021-30261  Possible integer and heap overflow due to lack of input command https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin									
qca6428_firm	iware								
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976									
qca6430_firm	ıware		GVE ID . GVE-2021-17/0						
CVSS Scoring Sca		1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1878
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1879
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1880

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID		Patch	NCIIPC ID
qca6431_firm	ıware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivit Snapdragon Industrial IC Snapdragon Wearables  CVE ID: CVE-2021-193	ht w co	attps://ww v.qualcomm. om/compan /product- ecurity/bull tins/august 2021- pulletin	0-QUA-QCA6- 061021/1881
Improper Input Validation	17-Sep-21	7.2	Possible integer and head overflow due to lack of it command size validation while handling beacon template update command from HLOS in Snapdragon Constitution, Snapdragon Industri IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-302	nput n ht and con umer rial et -2 sic,	attps://ww v.qualcomm. om/compan /product- ecurity/bull tins/august 2021- pulletin	0-QUA-QCA6- 061021/1882
qca6436_firm	ware					
NULL Pointer Dereference	17-Sep-21	4.9	preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,		attps://ww v.qualcomm. om/compan /product- ecurity/bull tins/august 2021- oulletin	0-QUA-QCA6- 061021/1883
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5		6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-QCA6- 061021/1884
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-QCA6- 061021/1885
qca6438_firm					
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-QCA6- 061021/1886

2-3 3-4 4-5

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Free 17-Sep-21 10 Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables CVE ID: CVE-2021-30261  Qca6564a_firmware  A use after free can occur due to improper validation of P2P device address in PD Request  Notation of 17-Sep-21 10 Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-30261 O-QUA-QCA6-0-QCA6-0-QUA-QCA6-0-QCA6-0-QCA6-0-QCA6-0-QCA6-0-QCA6-0-QUA-QCA6-0-QCA6-	Weakness	· · · · · · · · · · · · · · · · · · ·									
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Music, Snapdragon Wired Infrastructure and Networking   CVE ID : CVE-2021-1976   CVE ID : CVE											
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Wared Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command from HLOS in Snapdragon Ionsumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Ion Snapdragon Ion Summer IOT, Snapdragon Ion Summer IOT, Snapdragon Wareables (CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Ion Wareables (CVE ID: CVE-2021-30261)  Tribut  Validation  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Conne				<u> </u>							
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wered Infrastructure and Networking  CVE ID : CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon Weiral IOT, Snapdragon IoT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Weiralle IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Weiralle IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Weiralbes  CVE ID : CVE-2021-30261  Qca6564a_firmware  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Auto, Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, Snapdragon Compu				CVE ID : CVE-2021-1976							
to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID : CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IOT, Snapdragon IOT, Snapdragon IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID : CVE-2021-30261  Qca6564a_firmware  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Auto, Snapdragon Auto, Snapdragon Auto, Snapdragon Auto, Snapdragon Connectivity.  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Connectivity.  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Connectivity.  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Connectivity.  B ttps://ww w.qualcomm.com/compan y/product-security/bull etins/august	qca6564au_fi	qca6564au_firmware									
Improper Input Validation  Improper Input Validation  Input Validation  Input Validation  Improper Input Validation  Input		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	O-QUA-QCA6- 061021/1887					
Improper Input Validation Validation  IT-Sep-21  IT-Sep-2				CVE ID : CVE-2021-1976							
Use After Free  A use after free can occur due to improper validation of P2P w.qualcomm. device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, etins/august  A use after free can occur due https://ww w.qualcomm. com/compan y/product-security/bull etins/august	Improper Input Validation  17-Sep-21  7.2  7.2  Overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables CVE ID: CVE-2021-30261  Overflow due to lack of input command https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin										
Use After Free  17-Sep-21  10  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,  to improper validation of P2P w.qualcomm. com/compan y/product-security/bull etins/august	qca6564a_firmware										
CVSS Scoring Scale		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	w.qualcomm. com/compan y/product- security/bull	0-QUA-QCA6- 061021/1889					
	CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10					

Validation    Total Computed Nation   Security   Securi	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID				
Improper Input 17-Sep-21 7.2 Auto, Snapdragon Consumer IOT, Snapdragon Wearables CVE ID : CVE-2021-30261  Use After Free 17-Sep-21 17-Sep-21 10 Snapdragon Consumer IOT-Sep-21 10 Snapdragon Consumer IOT-Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-30261 10 Snapdragon Consumer IOT-Snapdragon Wearables CVE ID : CVE-2021-30261 10 Snapdragon Consumer IOT-Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1976 10 CVE-2021-1976				Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking						
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin	Input Validation	·	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	0-QUA-QCA6- 061021/1890				
to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking    Total Parametric in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking   CVE ID : CVE-2021-1976	qca6564_firm	iware								
45.0 04 40		Use After Free  17-Sep-21  10  device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  device address in PD Request frame in Snapdragon Auto, Mttps://www.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin  https://www.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin								
NIII 17-Sen-21 49 N. II	qca6574au_firmware									
NULL 17-36P-21 Null pointer dereference https://ww 0-QUA-QCA	NULL	NULL 17-Sep-21 4.9 Null pointer dereference https://ww 0-QUA-QCA6-								

validation when the preemption feature enablement is toggled in Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID : CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID : CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon industrial IOT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Mobile, Snapdragon Wearables  CVE ID : CVE-2021-30261  Improper Input  Validation  Validation	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon IoT, Snapdragon W., qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin  to improper validation of P2P device address in PD Request frame in Snapdragon IoT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	Pointer Dereference	preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939									
Improper Input Validation  17-Sep-21  7.2  7.2  7.2  Overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables CVE ID: CVE-2021-30261  O-QUA-QCA6-061021/1894  O-QUA-QCA6-061021/1894	Use After Free	device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin									
	Improper Input Validation	Improper Input Validation Validation  17-Sep-21  7.2  Overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  O-QUA-QCA6-061021/1894									
CVCC Sequing Scale 0.1 1.2 2.2 2.4 4.5 5.6 6.7 7.0 0.10	qca6574a_firmware										
	CVSS Scoring Sca		1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10					

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1895
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1896
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1897

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
qca6574_firm	ware					
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1898	
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID : CVE-2021-1976						
Improper Input Validation Validation  17-Sep-21  The proper Input Validation Validation  Improper Input Validation Validation  17-Sep-21  Improper Input Validation Validation  Improper Input Validation Validation  Improper Input Validation  Input						
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Descrip	tion & CVE	ID	Pa	Patch		IPC ID
			CVE ID : CVI	E-2021-3	0261				
qca6584au_fi	rmware								
Use After Free	17-Sep-21	10	A use after for to improper device address frame in Snar Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Infrastructur Networking	validationess in PD I pdragon A Compute Connectiv Consume Industria Voice & M Wearable Wired	n of P2P Request Auto, , vity, r IOT, I IOT, Iusic,	w.qual com/c y/prod securit etins/a -2021-	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		A-QCA6- 21/1901
			CVE ID : CVI	E-2021-1	976				
Improper Input Validation	17-Sep-21	7.2	Possible intervented overflow duction duction overflow du	e to lack of the total control	of input ion n nand agon sumer strial fusic,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		_	A-QCA6- 21/1902
qca6584_firm	qca6584_firmware								
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		_	A-QCA6- 21/1903	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6595au_fi  NULL Pointer Dereference		4.9	Snapdragon Mobile, Snapdragon Voice & Music Snapdragon Wearables  CVE ID: CVE-2021-3026  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IO' Snapdragon Industrial IO'	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	O-QUA-QCA6- 061021/1904
			Snapdragon Wearables  CVE ID: CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur of to improper validation of I device address in PD Requireme in Snapdragon Auto Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IO Snapdragon Industrial IO Snapdragon Voice & Music Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6- 061021/1905
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of inp command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industria	com/compan y/product- security/bull etins/august -2021-	0-QUA-QCA6- 061021/1906
CVSS Scoring Sca	le 0-1	1-2	<b>2-3 3-4 4-5 5</b>	<del>-6</del> 6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
qca6595_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA6- 061021/1907
qca6694au_fii	rmware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA6- 061021/1908
qca6694_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://ww w.qualcomm. com/compan	0-QUA-QCA6- 061021/1909
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	y/product- security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA6- 061021/1910
qca6696_firm	iware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6- 061021/1911
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P	https://ww w.qualcomm.	0-QUA-QCA6- 061021/1912
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	com/compan y/product- security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA6- 061021/1913
qca7500_firm	iware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA7- 061021/1914

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
qca7520_firm	iware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA7- 061021/1915
qca7550_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA7- 061021/1916
qca8072_firm	iware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	0-QUA-QCA8- 061021/1917
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	-2021- bulletin	
qca8075_firm	Iwaro		CVE ID : CVE-2021-1976		
qcaou/5_IIIII	Iware		A C. C.	T	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA8- 061021/1918
qca8081_firm	ıware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA8- 061021/1919

6-7

7-8

8-9

9-10

1-2

0-1

Use After Free  17-Sep-21  Use After Free  17-Sep-21  17-Sep-21  Use After Free  17-Sep-21  10  Use After Free  17-Sep-21  10  Use After Free  17-Sep-21  Industrial IOT, Snapdragon com/compan Wearables, Snapdragon etins/august -2021-bulletin  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Compute, Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables, -2021-	CID
Use After Free  17-Sep-21  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Auto, Snapdragon Compute, Snapdragon Auto, Snapdragon Compute, Snapdragon Wised Infrastructure, Snapdragon Wised Infrastructure, Snapdragon Wired Infrastructure, and Networking CVE ID: CVE-2021-1947  17-Sep-21  10    kernel graphics driver because of storing an invalid pointer in Snapdragon w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin    bulletin   https://ww y/product-security/bull etins/august   https://ww w.qualcomm. com/compan y/product-security/bull etins/august   https://ww w.qualcomm. com/com/com/com/com/com/com/com/com/com/	
Use After Free  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, https://ww w.qualcomm. com/compan y/product- security/bull 061021/1	-
Snapdragon Wired Infrastructure and Networking  CVE ID : CVE-2021-1976	-
qca9367_firmware	
Use After Free  17-Sep-21  10  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired  A use after free can occur due to improper validation of P2P device address in PD Request w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin	-
CVSS Scoring Scale	9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Infrastructure and Networking							
			CVE II	D : CVE-	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261				_	comm. compan luct- cy/bull nugust	_	A-QCA9- 21/1923
			CVE II	D : CVE-	2021-30	0261				
qca9377_firm	ware									
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	ointer d s due to tion who ption fe ement is ragon A ragon C ragon C ragon C ragon C ragon C ragon C	imprope en the ature toggled uto, ompute, onnectiv onsume industrial	in rity, r IOT, IOT, s	_	comm. ompan luct- y/bull nugust	_	A-QCA9- 21/1924
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,			•	comm. ompan luct- y/bull nugust	_	A-QCA9- 21/1925	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1926
qca9379_firm	iware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1927
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1928

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261		
qca9531_firm	ıware		CVE ID . CVE 2021 30201		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1929
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1930
qca9558_firm	iware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	0-QUA-QCA9- 061021/1931

6-7

7-8

8-9

9-10

2-3 3-4 4-5

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	-2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1932
qca9561_firm	lware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1933
Use After Free  CVSS Scoring Sca	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	O-QUA-QCA9- 061021/1934

Use After Free 17	are 7-Sep-21	7.2	Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon	-2021- bulletin https://ww w.qualcomm.	
Use After		7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon	_ ,,	
L 17	7-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon	_ ,,	
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947	com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1935
Use After Free 17	7-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1936
qca9880_firmwa	are				
Use After Free 17	7-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver	https://ww w.qualcomm.	0-QUA-QCA9- 061021/1937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	com/compan y/product- security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9- 061021/1938
qca9882_firm	iware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA9- 061021/1939
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P	https://ww w.qualcomm.	0-QUA-QCA9- 061021/1940
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	com/compan y/product- security/bull etins/august -2021- bulletin	
qca9886_firm	iware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA9- 061021/1941
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1942
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Use After Free   17-Sep-21   17-Sep-21   18   2	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free  17-Sep-21  7.2    Total Compute   Shapdragon   Compute   Shapdragon   Compute   Shapdragon   Compute   Shapdragon   Compute   Comp	qca9887_firm	iware				
Use After Free  IT-Sep-21  IT-Sep		17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	
Use After Free  17-Sep-21  7.2  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and  Use After Free  17-Sep-21  7.2  Use-after-free vulnerability in kernel graphics driver because of storing an invalid w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	
Use After Free  17-Sep-21  7.2    kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and   https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin   0-QUA-QCA9-061021/1945   0-QUA-QCA9-	qca9888_firm	iware				
		17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA9- 061021/1946
			CVE ID : CVE-2021-1976		
qca9889_firm	iware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA9- 061021/1947
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1948
	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and		
			Networking		
			CVE ID : CVE-2021-1976		
qca9896_firm	iware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1949
			CVE ID: CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA9- 061021/1950
qca9898_firm	iware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	0-QUA-QCA9- 061021/1951
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 725 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	bulletin	
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1952
qca9980_firm	ıware		CVEID: CVE 2021 1770		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1953
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	0-QUA-QCA9- 061021/1954

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	bulletin	
qca9982_firm	ware		CVEID: CVE 2021 1770		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9- 061021/1955
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA9- 061021/1956
qca9984_firm					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid	https://ww w.qualcomm. com/compan	0-QUA-QCA9- 061021/1957
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 Page 727 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	y/product- security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1958
qca9985_firm	iware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA9- 061021/1959
qca9986_firm	ıware		2.2.2.2.2.2.2.2.2.7.0		
CVSS Scoring Sca		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1960
qca9987_firm	ıware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA9- 061021/1961
qca9988_firm	ıware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-QCA9- 061021/1962
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976		
qca9990_firm	ıware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-QCA9- 061021/1963
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-QCA9- 061021/1964
qca9992_firm					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull	O-QUA-QCA9- 061021/1965

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	etins/august -2021- bulletin	
			CVE ID: CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCA9- 061021/1966
qca9994_firm	ware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCA9- 061021/1967
Use After Free  CVSS Scoring Sca	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,  2-3 3-4 4-5 5-6	https://www.qualcomm.com/company/product-security/bull	0-QUA-QCA9- 061021/1968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	etins/august -2021- bulletin				
qcm2290_firm	nware							
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- QCM2- 061021/1969			
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- QCM2- 061021/1970			
qcm4290_firm	qcm4290_firmware							
Use After	17-Sep-21	7.2	Use-after-free vulnerability in	https://ww	O-QUA-			
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 Page 732 of 861	6-7 7-8	8-9 9-10			

pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Merarables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1947  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Moice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-30261	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woile, Snapdragon Voice & Music, Snapdragon Noice, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	Free			because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	com/compan y/product- security/bull etins/august -2021-	QCM4- 061021/1971
Improper Input Validation Validat		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	_
	Input	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	_
qcm6125_firmware	qcm6125_firr	nware		C. 2.2. C. 2 2021 00201		
	•		4.3		6.7	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- QCM6- 061021/1974
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- QCM6- 061021/1975
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- QCM6- 061021/1976

6-7

7-8

8-9

9-10

2-3 3-4 4-5

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Des	cription & (	CVE ID		Pa	tch	NCI	IPC ID
qcn3018_firm	iware									
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976				com/c	comm. ompan luct- cy/bull august	_	A-QCN3- 1/1977
qcn5021_firm	ıware		CVETET	0.5 -0-1						
	A use after free can occur due									
Use After Free	17-Sep-21	10	device ad frame in S Snapdrag Snapdrag Snapdrag Snapdrag Snapdrag Snapdrag Snapdrag Infrastruc	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		_	comm. ompan luct- cy/bull august	_	A-QCN5- 1/1978	
qcn5022_firm	iware									
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,		com/c	comm. ompan luct- cy/bull august	_	A-QCN5- 1/1979		
CVSS Scoring Sca	le <b>0-1</b>	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		
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	bulletin			
qcn5024_firm	lware		CVE ID . CVE-2021-17/0				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCN5- 061021/1980		
qcn5052_firm	iware						
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCN5- 061021/1981		
qcn5054_firmware							
Use After	17-Sep-21	10	A use after free can occur due	https://ww	O-QUA-QCN5-		

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/1982
qcn5064_firm	ıware				
Use After Free	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,		Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCN5- 061021/1983
qcn5121_firm	iware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCN5- 061021/1984
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
			Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976					
qcn5122_firm	iware							
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCN5- 061021/1985			
qcn5124_firm	iware							
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCN5- 061021/1986			
qcn5152_firmware								
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://ww w.qualcomm. com/compan	0-QUA-QCN5- 061021/1987			
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	y/product- security/bull etins/august -2021- bulletin	
qcn5154_firm	ıware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCN5- 061021/1988
qcn5164_firm	iware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCN5- 061021/1989
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1976		
qcn5500_firm	ıware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-QCN5- 061021/1990
qcn5502_firm	ıware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCN5- 061021/1991
qcn5550_firm	iware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcomm. com/compan y/product- security/bull	O-QUA-QCN5- 061021/1992
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	De	escriptio	n & CVE	ID	Pa	tch	NCI	IPC ID
			Snapdra Snapdra Snapdra Snapdra Infrastra Network	Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976				august n		
qcn6023_firmware										
Use After Free	17-Sep-21	10	A use afto improdevice a frame in Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra Snapdra CVE ID	oper valdress on Snape on Co on Son Co on Son Co on Son Wo on Wo o	alidations in PD Formpute, connective consumerations & March 2016 & Ma	a of P2P Request Auto, rity, r IOT, I IOT, Iusic, s,	com/c y/prod securit	comm. ompan duct- ty/bull august	_	A-QCN6- 1/1993
qcn6024_firm	iware									
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976			com/c y/prod securit	ompan duct- ty/bull august	_	A-QCN6- 1/1994	
			( ,	: (:VE-:	2()21-19	1/D				

Weakness	Publish Date	CVSS	Descript	ion & CVE	ID	Pa	tch	NCI	IPC ID
qcn6122_firm	iware								
Use After Free	17-Sep-21	10	A use after from to improper to improper to device address frame in Snap Snapdragon (Snapdragon (Snapd	com/c	comm. ompan luct- cy/bull nugust	_	A-QCN6- 21/1995		
qcn9000_firm	ware		CVE ID . CVE	2021 1.					
			A use after fr						
Use After Free	17-Sep-21	10	device address frame in Snap Snapdragon ( Snapdragon ( Sn	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and		_	comm. ompan luct- cy/bull august	_	A-QCN9- 21/1996
qcn9012_firm	iware								
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,		com/c	comm. ompan luct- cy/bull nugust	_	A-QCN9- 21/1997	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	bulletin			
qcn9022_firm	l ware		012121 012 2021 1970				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCN9- 061021/1998		
qcn9024_firm	ıware						
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCN9- 061021/1999		
qcn9070_firmware							
Use After	17-Sep-21	10	A use after free can occur due	https://ww	O-QUA-QCN9-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/2000
qcn9072_firm	ıware				
Use After Free	device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,		to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCN9- 061021/2001
qcn9074_firm	iware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCN9- 061021/2002
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976		
qcn9100_firn	iware			1	1
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCN9- 061021/2003
qcs2290_firm	iware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCS2- 061021/2004
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	0-QUA-QCS2- 061021/2005

6-7

7-8

8-9

9-10

2-3 3-4 4-5

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	-2021- bulletin	
qcs405_firmv	varo		CVE ID : CVE-2021-1976		
qcs405_mmv	vare		A C. C.	T	Г
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCS4- 061021/2006
qcs410_firmv	vare				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCS4- 061021/2007

6-7

7-8

8-9

9-10

2-3 3-4 4-5

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCS4- 061021/2008
1000 0			CVE ID : CVE-2021-30261		
qcs4290_firm	ware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCS4- 061021/2009
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCS4- 061021/2010

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			Networking					
			CVE ID: CVE-2021-1976					
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCS6- 061021/2014			
qcs605_firmware								
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCS6- 061021/2015			
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCS6- 061021/2016			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			Infrastructure and Networking						
			CVE ID : CVE-2021-1976						
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-QCS6- 061021/2017				
			CVE ID : CVE-2021-30261						
qcs610_firmv	qcs610_firmware								
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCS6- 061021/2018				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCS6- 061021/2019				
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Description & CVI	: ID	Patch	NCII	PC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & M Snapdragon Wearable	es			
6.4.0 M C			CVE ID : CVE-2021-3	0261			
qcs6125_firm	ware			1.11.			
Use After Free	17-Sep-21	7.2	Use-after-free vulnerakernel graphics drive because of storing an pointer in Snapdrago Compute, Snapdrago Connectivity, Snapdra Industrial IOT, Snapd Mobile, Snapdragon Wearables, Snapdrago Wired Infrastructure Networking	invalid httm w. congon y/ ragon secuent	etps://ww .qualcomm. om/compan /product- ecurity/bull ins/august :021- ulletin	•	1-QCS6- 1/2020
			CVE ID : CVE-2021-1	947			
Use After Free	17-Sep-21	10	A use after free can of to improper validation device address in PD frame in Snapdragon Snapdragon Computer Snapdragon Connection Snapdragon Consumers Snapdragon Industriated Snapdragon Wearable Snapdragon Wearable Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1	n of P2P Request Auto, htt , w. vity, co er IOT, y/ sel Music, eti es, -20	ctps://ww .qualcomm. om/compan /product- ecurity/bull ins/august :021- ulletin	•	a-QCS6- 1/2021
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer		ctps://ww .qualcomm. om/compan /product- ecurity/bull ins/august		1-QCS6- 1/2022
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5</b>	5-6 6-	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	bulletin			
qcx315_firmware							
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QCX3- 061021/2023		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QCX3- 061021/2024		
qet4101_firm	ware						
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the	https://ww w.qualcomm. com/compan	0-QUA-QET4- 061021/2025		
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	y/product- security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QET4- 061021/2026
qrb5165_firm	iware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QRB5- 061021/2027
Use After Free  CVSS Scoring Sca	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute,  2-3 3-4 4-5 5-6	https://ww w.qualcomm. com/compan y/product- security/bull	0-QUA-QRB5- 061021/2028

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID							
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	etins/august -2021- bulletin								
qsm8250_firm	nware											
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-QSM8- 061021/2029							
qsw8573_firm	ıware											
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- QSW8- 061021/2030							
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid	https://ww w.qualcomm. com/compan	O-QUA- QSW8- 061021/2031							
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8								

Improper Input 17			pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947 Possible integer and heap	y/product- security/bull etins/august -2021- bulletin	
1			Possible integer and heap		
Validation	7-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- QSW8- 061021/2032
qualcomm215_fi	firmware				
NULL Pointer 17 Dereference	7-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-QUAL- 061021/2033
Use After Free 17	7-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product-	0-QUA-QUAL- 061021/2034

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan	O-QUA-QUAL- 061021/2035
sa415m_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur du to improper validation of P2 device address in PD Reques frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	P	0-QUA-SA41- 061021/2036
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-SA41-
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/2037
sa515m_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SA51- 061021/2038
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SA51- 061021/2039

6-7

2-3 3-4 4-5

1-2

0-1

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
sa6145p_firm	ware			1	<u> </u>
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SA61- 061021/2040
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SA61- 061021/2041
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SA61- 061021/2042
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Snapd	ragon W	/earable	es				
			CVE II	D : CVE-	2021-3	0261				
sa6150p_firm	ware									
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	ointer d due to tion who ption fe ement is ragon C ragon C ragon C ragon Ir ragon W C C: CVE-	imprope en the ature toggled uto, ompute, onnectiv onsume idustria	in vity, r IOT, l IOT,	_	comm. ompan luct- cy/bull august	_	A-SA61- 21/2043
Use After Free	17-Sep-21	10	to imp device frame Snapd Snapd Snapd Snapd Snapd Snapd Infras	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			•	comm. ompan luct- cy/bull august	_	A-SA61- 21/2044
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,			_	comm. ompan luct- cy/bull august	_	A-SA61- 21/2045	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	De	escriptio	on & CVE	ID	Pa	tch	NCI	IPC ID
			Snapdra	_						
			Snapdra							
			CVE ID	: CVE-2	2021-30	)261				
sa6155p_firm	ware		T				T		ı	
NULL Pointer Dereference	17-Sep-21	4.9	Null por occurs of validati preemp enabler Snapdra Snapdra Snapdra Snapdra Snapdra	due to i on whe otion fe ment is agon Co agon Co agon In agon W	imprope en the ature toggled uto, ompute, onnective onsume idustrial	in vity, r IOT, l IOT, s	_	comm. compan luct- cy/bull nugust	_	A-SA61- 21/2046
			CVE ID	: CVE-2	2021-19	939				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		_	comm. ompan luct- y/bull nugust	_	A-SA61- 21/2047		
			CVE ID	: CVE-2	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,			_	comm. ompan luct- y/bull nugust	_	A-SA61- 21/2048	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
sa6155_firmv	vare		Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261		
			Null pointer dereference		
NULL Pointer Dereference	17-Sep-21	4.9	occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SA61- 061021/2049
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2E device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		0-QUA-SA61- 061021/2050
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	com/compan y/product- security/bull etins/august	0-QUA-SA61- 061021/2051
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Desc	cription & C	VE ID	Pa	tch	NCI	IPC ID
			Snapdrag Snapdrag Snapdrag	odragon Ioʻ gon Mobile gon Voice & gon Wearal CVE-2021	Music, bles				
sa8145p_firm	ware		CVEID:	CVE-2021	-30201				
NULL Pointer Dereference	17-Sep-21	4.9	occurs du validatior preempti- enableme Snapdrag Snapdrag Snapdrag Snapdrag Snapdrag Snapdrag	gon Compugon Connection gon Consurgon Industr gon Wearal	ed in te, ctivity, mer IOT, rial IOT,	com/c y/prod	comm. ompan duct- ty/bull august	_	a-SA81- 1/2052
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976			com/c y/prod	comm. ompan duct- ty/bull august	_	a-SA81- 1/2053
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer			com/c y/prod	comm. ompan duct- ty/bull august	_	A-SA81- 1/2054
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description	n & CVE ID	Patc	h	NCI	PC ID
			IOT, Snapdrago IOT, Snapdrago Snapdragon Mo Snapdragon Vo Snapdragon Wo CVE ID: CVE-2	on IoT, obile, oice & Music, earables	bulletin			
sa8150p_firm	ıware							
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer de occurs due to in validation when preemption fea enablement is to Snapdragon Conspandragon Conspandragon Conspandragon Conspandragon Inconspandragon Weller CVE ID: CVE-2	mproper in the ature toggled in ato, ampute, annectivity, ansumer IOT, dustrial IOT, earables	https://w.qualcocom/cory/produsecurity/etins/au-2021-bulletin	omm. npan ct- /bull	_	a-SA81- 1/2055
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		•	omm. npan ct- /bull	_	1-SA81- 1/2056
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon https://ww w.qualcomm. com/compan y/product-security/bull etins/august			_	1-SA81- 1/2057	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	-2021- bulletin	
sa8155p_firm	ıware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SA81- 061021/2058
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SA81- 061021/2059
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://ww w.qualcomm. com/compan y/product- security/bull	0-QUA-SA81- 061021/2060

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	etins/august -2021- bulletin	
sa8155_firmw	vare				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SA81- 061021/2061
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SA81- 061021/2062
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://ww w.qualcomm. com/compan y/product-	0-QUA-SA81- 061021/2063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	security/bull etins/august -2021- bulletin	
sa8195p_firm	ware				1
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SA81- 061021/2064
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SA81- 061021/2065
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://ww w.qualcomm. com/compan	0-QUA-SA81- 061021/2066
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	y/product- security/bull etins/august -2021- bulletin	
sc8180x\\+sc	dx55_firmwa	re			
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SC81- 061021/2067
sd205_firmwa	are				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD20- 061021/2068
Use After	17-Sep-21	10	A use after free can occur due	https://ww	O-QUA-SD20-

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/2069
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD20- 061021/2070
sd210_firmwa	are				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD21- 061021/2071
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SD21- 061021/2072
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SD21- 061021/2073
sd429_firmwa	are				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD42- 061021/2074
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 769 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD42- 061021/2075
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD42- 061021/2076
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD42- 061021/2077

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30261		
sd439_firmwa	are			<u> </u>	1
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SD43- 061021/2078
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD43- 061021/2079
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD43- 061021/2080
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			Snapd	ragon W	/earable	es				
			CVE II	D : CVE-	2021-3	0261				
sd450_firmwa	are									
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd			comm. ompan luct- cy/bull august	_	A-SD45- 21/2081		
Use After Free	17-Sep-21	10	to impose devices frame Snapd Snapd Snapd Snapd Snapd Infras	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		_	A-SD45- 21/2082	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		0-QUA-SD45- 061021/2083			
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music,		
			Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
sd460_firmwa	are				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD46- 061021/2084
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SD46- 061021/2085
sd480_firmwa	are				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	0-QUA-SD48- 061021/2086

6-7

7-8

8-9

9-10

2-3 3-4 4-5

1-2

0-1

CVSS Scoring Scale

Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity Weather in PD Request frame in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables CVE ID: CVE-2021-30261  sd632_firmware  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragons Auto,  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,  Null etins/august O-QUA-SD63- 061021/2089	Weakness	Publish Date	CVSS	Description	on & CVE	ID	Pat	ch	NCI	IPC ID
A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking  CVE ID : CVE-2021-1976  Possible integer and heap overflow due to lack of input command from HLOS in Snapdragon Waqualcomm. Com/compan y/product-security/bull etins/august -2021-bulletin  17-Sep-21  Improper Input Validation  Improper Validation  17-Sep-21  Improper Input Validation  Improper Validation  Improper Input Validation  IT-Sep-21  IT-S				Snapdragon C Snapdragon Ir Snapdragon W	onsume Idustrial Jearable	r IOT, IOT, s	bulletii	1		
Improper Input Validation Validation  Improper Input Validation Validation  Improper Input Validation Validation  IT-Sep-21  IT-Sep-		17-Sep-21	10	A use after free to improper volume address frame in Snaperagon Consumer Snaperagon Consumer Snaperagon Volume Snaperagon Work	e can occalidation in PD R dragon A ompute, onnective onsumendustrial oice & M Vearable and	cur due of P2P Request Auto, rity, r IOT, IOT, lusic, s,	w.quale com/co y/prod securit etins/a -2021-	comm. ompan uct- y/bull ugust	_	
NULL Pointer Dereference  17-Sep-21 Dereferen	Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		w.quale com/ce y/prod securit etins/a -2021-	comm. ompan uct- y/bull ugust	_		
NULL Pointer Dereference  17-Sep-21 Dereferen	sd632_firmwa	are								
	Pointer Dereference			occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,		w.qualcomm. com/compan y/product- security/bull		06102	1/2089	

Weakness	Publish Date	cvss	Descriptio	n & CVE ID		Pat	ch	NCI	IPC ID
			Snapdragon Co Snapdragon Co Snapdragon In Snapdragon W CVE ID : CVE-2	onnectivity onsumer IO dustrial IO earables	ОТ, ОТ,	-2021- bulleti	1		
Use After Free	17-Sep-21	10	A use after free to improper var device address frame in Snape Snapdragon Co Snapdragon Co Snapdragon In Snapdragon W Snapdragon W Snapdragon W Infrastructure Networking CVE ID: CVE-2	alidation of the state of the s	f P2P quest to, y, OT, OT, sic,	https:/ w.qual com/co y/prod securit etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	_	A-SD63- 1/2090
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261		https:/ w.qual com/co y/prod securit etins/a -2021- bulletin	comm. ompan uct- y/bull ugust		A-SD63- 1/2091	
sd660_firmwa	are								
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon		https:/ w.qual com/co y/prod securit	comm. ompan uct-	_	A-SD66- 1/2092	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	etins/august -2021- bulletin	
			CVE ID: CVE-2021-1947		
sd662_firmwa	are				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD66- 061021/2093
			A use after free can occur due		
Use After Free	17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD66- 061021/2094
			CVE ID : CVE-2021-1976		
sd665_firmwa	are				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the	https://ww w.qualcomm. com/compan	0-QUA-SD66- 061021/2095
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 776 of 861	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	y/product- security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD66- 061021/2096
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD66- 061021/2097
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon	https://ww w.qualcomm. com/compan y/product-	0-QUA-SD66- 061021/2098

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	security/bull etins/august -2021- bulletin	
sd670_firmwa	are				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD67- 061021/2099
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD67- 061021/2100
Improper Input Validation CVSS Scoring Sca	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation  2-3 3-4 4-5 5-6	https://ww w.qualcomm. com/compan	0-QUA-SD67- 061021/2101 8-9 9-10

Weakness	Publish Date	cvss	Description & C	VE ID	Pat	ch	NCI	IPC ID
			while handling beatemplate update confrom HLOS in Snap Auto, Snapdragon (IOT, Snapdragon In IOT, Snapdragon Mobile Snapdragon Voice Snapdragon Weara CVE ID: CVE-2021	y/prod security etins/a -2021- bulletin	y/bull ugust			
sd675_firmwa	are							
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer derefe occurs due to improvalidation when the preemption feature enablement is togg Snapdragon Auto, Snapdragon Compu Snapdragon Conne Snapdragon Consul Snapdragon Indust Snapdragon Weara	oper e led in lete, ctivity, mer IOT, rial IOT,	https://w.quald.com/co y/prod security etins/a -2021- bulletir	comm. ompan uct- y/bull ugust	_	A-SD67- 21/2102
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		https://w.qualocom/com/coy/prodsecurityetins/a-2021-bulletir	comm. ompan uct- y/bull ugust	_	A-SD67- 21/2103
Improper Input	17-Sep-21	7.2	Possible integer an overflow due to lac		https://www.qualcomm.		0-QUA-SD67- 061021/2104	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE II	)	Pat	ch	NCI	IPC ID
Validation			command size validation while handling beacon template update commands from HLOS in Snapdrage Auto, Snapdragon Construction, Snapdragon Industruction, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Muscon Snapdragon Wearables CVE ID: CVE-2021-302	and on umer crial	com/co y/prod securit etins/a -2021- bulletin	luct- y/bull nugust		
sd678_firmwa	are		N. 11				I	
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity Snapdragon Industrial I Snapdragon Wearables CVE ID: CVE-2021-193	https://w.qual com/co y/prod securit etins/a -2021- bulletin	comm. ompan luct- y/bull nugust	_	A-SD67- 1/2105	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976		https:/ w.qual com/co y/prod securit etins/a -2021- bulletin	comm. ompan luct- y/bull nugust	_	A-SD67- 1/2106
Improper	17-Sep-21	7.2	Possible integer and he		https:/	/ww	0-0114	A-SD67-
CVSS Scoring Sca	_	1-2	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	NCI	IPC ID	
Input Validation			overflow due to lack of inportant command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumplot, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	com/co y/prode security etins/as er -2021- l bulletin	ompan uct- y/bull ugust	06102	21/2107	
sd690_5g_firm	nware							
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT Snapdragon Industrial IOT Snapdragon Wearables	_	omm. ompan uct- y/bull ugust	_	A-SD69- 21/2108	
			CVE ID : CVE-2021-1939					
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability kernel graphics driver because of storing an invalipointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	id https:// w.qualc com/co y/prod	omm. ompan uct- y/bull ugust	_	A-SD69- 21/2109	
Use After Free	17-Sep-21	10	A use after free can occur d to improper validation of P		https://ww w.qualcomm.		0-QUA-SD69- 061021/2110	
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-</b>	6 6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	com/compan y/product- security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD69- 061021/2111
sd712_firmwa	are				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD71- 061021/2112
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
sd720g_firmv	vare				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD72- 061021/2113
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD72- 061021/2114
sd730_firmwa	are			l	
NULL Pointer Dereference 17-Sep-21 4.9		4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD73- 061021/2115
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Desc	ription & CVE	ID	Pa	tch	NCI	IPC ID
			Snapdrago	on Wearable	S				
			CVE ID : C	VE-2021-19	939				
Use After Free	17-Sep-21	10	device add frame in S Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Snapdrago Infrastruc	evice address in PD Request rame in Snapdragon Auto, napdragon Compute, napdragon Consumer IOT, napdragon Industrial IOT, napdragon Voice & Music, napdragon Wearables, napdragon Wired afrastructure and letworking  EVE ID: CVE-2021-1976  https://www.qualcomm.com/company/product-security/bull etins/august-2021-bulletin				_	A-SD73- 21/2116
			CVE ID : C	VE-2021-19	976				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			•	comm. ompan luct- cy/bull august	_	A-SD73- 21/2117
sd750g_firmv	vare								
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,			•	comm. ompan luct- cy/bull august	0-QUA-SD75- 061021/2118	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3	-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables		
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD75- 061021/2119
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD75- 061021/2120
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD75- 061021/2121
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			_	lragon V						
				lragon W						
			CVEII	D : CVE-	2021-30	0261				
sd765g_firmv	vare		1				T		T	
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  https://www.qualcomm.com/company/product-security/bull etins/august-2021-bulletin				comm. ompan luct- cy/bull nugust	_	A-SD76- 21/2122
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			•	comm. ompan luct- cy/bull nugust	_	A-SD76- 21/2123	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired			_	comm. ompan luct- cy/bull august	0-QUA-SD76- 061021/2124		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking CVE ID: CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD76- 061021/2125
sd765_firmw	are				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD76- 061021/2126
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD76- 061021/2127

Weakness	Publish Date	CVSS	Descripti	on & CVE	ID	Pa	tch	NCI	IPC ID
			Networking						
			CVE ID : CVE-	2021-19	947				
Use After Free	17-Sep-21	10	device addres frame in Snap Snapdragon C Snapdragon C Snapdragon I Snapdragon V Snapdragon V Snapdragon V	CVE ID : CVE-2021-1976			//ww comm. ompan duct- cy/bull august	_	A-SD76- 21/2128
			CVE ID : CVE-	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			•	comm. ompan luct- cy/bull august		A-SD76- 21/2129
sd768g_firmv	vare								
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin				
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD76- 061021/2131
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD76- 061021/2132
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD76- 061021/2133

**2-3 3-4 4-5** 

5-6

6-7

8-9

9-10

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
sd778g_firmv	varo		CVE ID : CVE-2021-30201		
Su / / Og_III III v	vai e		Null pointer dereference		
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD77- 061021/2134
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SD77- 061021/2135
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD77- 061021/2136

Signaphagon Mobile, Snapdragon Weice & Music, Snapdragon Wearables CVE ID : CVE-2021-30261  Sd780g_firmware  NULL  NULL  Pointer Dereference  17-Sep-21  Use After Free  17-Sep-21  17-Sep-21  Sapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wearables, Snapdragon	Weakness	Publish Date	cvss	Description	& CVE ID	Patc	h	NCI	IPC ID
NULL Pointer Dereference  17-Sep-21  4.9  4.9  4.9  4.9  4.9  4.9  Ause after free can occur due to improper validation when the preemption feature enablement is toggled in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mutstrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon industrial  17-Sep-21  Validation  Valida				Snapdragon Voic Snapdragon Wes	ce & Music, arables				
NULL Pointer Dereference Pointer Snapdragon Consumet IOT, Snapdragon Consumer IOT, Snapdragon Wearables CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Consumer IOT, Snapdrago	sd780g_firmv	vare							
to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking    Improper Input Validation   17-Sep-21   17-Sep-21   17-Sep-21   18-Sep-21   18-Sep-21   19-Sep-21   1	Pointer	17-Sep-21	4.9	occurs due to im validation when preemption feat enablement is to Snapdragon Aut Snapdragon Con Snapdragon Con Snapdragon Con Snapdragon Indi Snapdragon Wes	aproper the ure oggled in o, appute, anectivity, asumer IOT, ustrial IOT, arables	w.qualco com/con y/produ security etins/au -2021-	omm. mpan ict- /bull	_	
Improper Input Validation  17-Sep-21  Tolerand size validation Validation  17-Sep-21  Tolerand size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial  Auto Snapdragon Industrial  W.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		17-Sep-21	10	A use after free of to improper validevice address in frame in Snapdress Consumper Snapdragon Consumper Snapdragon Consumper Snapdragon Industry Snapdragon Wester Snapdragon Wir Infrastructure at Networking	w.qualco com/con y/produ security etins/au -2021-	omm. mpan ict- /bull			
	Input	17-Sep-21	7.2	overflow due to command size ver while handling be template update from HLOS in Sn Auto, Snapdragor IOT, Snapdragor	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer  w.qualcomm. com/compan y/product- security/bull etins/august -2021-			_	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-30261		
sd820_firmwa	are				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SD82- 061021/2140
sd821_firmwa	are				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD82- 061021/2141
ad025 5			CVE ID : CVE-2021-30261		
sd835_firmwa	are		A use after free can occur due	https://ww	
Use After Free	17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto,	w.qualcomm. com/compan y/product-	0-QUA-SD83- 061021/2142
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

		Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	security/bull etins/august -2021- bulletin	
17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD83- 061021/2143
re				
17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD84- 061021/2144
17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://ww w.qualcomm. com/compan	0-QUA-SD84- 061021/2145
	re 17-Sep-21	17-Sep-21 4.9 17-Sep-21 10	Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables CVE ID: CVE-2021-30261  Te  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Uearables CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request	Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261  Te  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Wearables CVE ID: CVE-2021-1939  A use after free can occur due to improper validation of P2P device address in PD Request  https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin  https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	y/product- security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD84- 061021/2146
sd850_firmwa	are				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD85- 061021/2147
sd855_firmwa	are				
CVSS Scoring Sca		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

NULL Pointer Dereference  17-Sep-21  Use After Free  17-Sep-21  17-Sep-21  Ive After Free  18-Sep-21  Ive After Free  Ive After Free	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free   17-Sep-21   10	Pointer	17-Sep-21	4.9	occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	
Use After Free  17-Sep-21  10  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  to improper validation of P2P device address in PD Request frame in Snapdragon Auto, https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin		17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	_
Improper 17-Sep-21 7.2 Possible integer and heap https://www. Ocollo-SD85-		17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	•
1 Ossible integer and neap   https://ww   O-QOA-5DO5-	Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-SD85-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	com/compan y/product- security/bull etins/august	061021/2151
sd865_5g_firm	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD86- 061021/2152
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability is kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947		0-QUA-SD86- 061021/2153
Use After Free	17-Sep-21	10	A use after free can occur du to improper validation of P2	1 //	0-QUA-SD86- 061021/2154
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	com/compan y/product- security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD86- 061021/2155
sd870_firmwa	are				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD87- 061021/2156
Use After	17-Sep-21	7.2	Use-after-free vulnerability in	https://ww	O-QUA-SD87-
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947  A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976  10 Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Worde Wusics, Snapdragon Mobile, Snapdragon Worde Wusics, Snapdragon Mobile, Snapdragon Worde Standard Wusics Snapdragon Worde Wusics Snapdragon Worde Wusics Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Worde Standard Wusics Snapdragon Worde S	Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976  Possible integer and heap overflow due to lack of input command from HLOS in Snapdragon Lonsumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking  The possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261  to improper validation of P2P device address in PD Request frame in Snapdragon O-QUA-SD87-061021/2159  to improper walldation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon wanter IOT, Snapdragon IoT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	Free			because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	com/compan y/product- security/bull etins/august -2021-	061021/2157
overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261  overflow due to lack of input command size validation https://ww w.qualcomm. com/compan y/product-security/bull etins/august -2021-bulletin	Use After Free	17-Sep-21	10	to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	_
	Improper Input Validation	17-Sep-21	7.2	overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	w.qualcomm. com/compan y/product- security/bull etins/august -2021-	_
	sd888_5g_firn	nware		3.21D 1 371 2021 30201		
	CVSS Scoring Sca		1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD88- 061021/2160
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD88- 061021/2161
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD88- 061021/2162

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
sd888_firmwa	are									
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd Snapd	s due to tion who ption fe ement is ragon C ragon C ragon C ragon Ir ragon W	ature toggled	in vity, r IOT, I IOT,	com/c	comm. ompan luct- cy/bull august	_	A-SD88- 21/2163
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976			com/c	comm. ompan luct- cy/bull august	_	A-SD88- 21/2164	
sda429w_firn	nware									
NULL Pointer Dereference	17-Sep-21	4.9	occurs valida preem enable Snapd Snapd Snapd Snapd Snapd	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables		com/c y/prod securit	comm. ompan luct- cy/bull nugust	_	A-SDA4- 21/2165	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon com/compan Connectivity, Snapdragon ground compute, Snapdragon hobile, Snapdragon ground compute, Snapdragon ground product security/bull etins/august wearables, Snapdragon -2021-	
kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wequalcomm. Com/compan y/product- security/bull off1021	
Wired Infrastructure and bulletin Networking	
CVE ID : CVE-2021-1947	
Improper Input Validation  17-Sep-21  Validation  Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261  Possible integer and heap overflow due to lack of input command size validation https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	
sdm429w_firmware	
NULL Pointer Dereference  17-Sep-21  Dereference  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	
CVSS Scoring Scale	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SDM4- 061021/2169
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SDM4- 061021/2170
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SDM4- 061021/2171

**2-3 3-4 4-5** 

1-2

0-1

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
sdm630_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SDM6- 061021/2172
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SDM6- 061021/2173
sdm830_firm	ware			l	
NULL Pointer Dereference  17-Sep-21 4.9		4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SDM8- 061021/2174
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pa	tch	NCI	IPC ID
			Snapdrag	gon W	'earable	S				
			CVE ID:	CVE-2	2021-19	939				
Use After Free	17-Sep-21	7.2	kernel gr because of pointer i Compute Connecti Industria Mobile, S Wearable Wired In	pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon				/ww comm. ompan luct- cy/bull august	_	A-SDM8- 21/2175
			CVE ID :	CVE-2	2021-19	947				
Use After Free	17-Sep-21	10	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,				_	comm. compan luct- cy/bull nugust	_	A-SDM8- 21/2176
sdw2500_firm	nware									
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,			_	comm. compan luct- cy/bull nugust	0-QUA SDW2 06102		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- SDW2- 061021/2178
sdx12_firmwa	are				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SDX1- 061021/2179
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer  2-3 3-4 4-5 5-6	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	0-QUA-SDX1- 061021/2180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	bulletin	
sdx20m_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SDX2- 061021/2181
sdx20_firmwa	are				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SDX2- 061021/2182
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://ww w.qualcomm.	0-QUA-SDX2- 061021/2183
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 806 of 861	6-7 7-8	8-9 9-10

Weakness	<b>Publish Date</b>	CVSS	Description & CVE ID		Pa	tch	NCI	IPC ID
Validation			command size validation while handling beacon template update comman from HLOS in Snapdragor Auto, Snapdragon Consur IOT, Snapdragon Industri IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Musi Snapdragon Wearables  CVE ID: CVE-2021-3026	com/com/com/com/com/com/com/com/com/com/	y/bull august			
sdx24_firmwa	ire			T				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IO Snapdragon Wearables  CVE ID: CVE-2021-1939	)Т, Т,	_	comm. ompan luct- cy/bull august	_	A-SDX2- 1/2184
Use After Free	17-Sep-21	10	A use after free can occur to improper validation of device address in PD Requirements in Snapdragon Auto Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IO Snapdragon Industrial IO Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	_	comm. ompan duct- cy/bull august	_	A-SDX2- 1/2185	
Improper	17-Sep-21	7.2	Possible integer and heap		https:/	 '/ww	0-011	A-SDX2-
CVSS Scoring Sca	_	1-2		5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/2186
sdx50m_firm	ware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5- 061021/2187
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5- 061021/2188

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	[	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			CVE II	) : CVE-	2021-30	0261				
sdx55m_firmv	ware						L			
NULL Pointer Dereference	17-Sep-21	4.9	occurs validat preem enable Snapd Snapd Snapd Snapd Snapd Snapd	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin					_	A-SDX5- 21/2189
Use After Free	17-Sep-21	7.2	kernel becaus pointe Compu Conne Indust Mobile Weara Wired Netwo	graphicse of sto r in Snaute, Snap ctivity, S rial IOT e, Snapd bles, Sn Infrastr	es driver ring an i pdragon odragon Snapdra , Snapdr ragon apdrago	nvalid gon agon n	com/c y/prod securi	comm. ompan duct- ty/bull august	_	A-SDX5- 21/2190
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			com/c y/prod securi	comm. ompan duct- ty/bull august	_	A-SDX5- 21/2191	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan	0-QUA-SDX5- 061021/2192
			CVE ID : CVE-2021-30261		
sdx55_firmwa	ire				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5- 061021/2193
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability is kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947		O-QUA-SDX5- 061021/2194
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SDX5- 061021/2195
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SDX5- 061021/2196
sdxr1_firmwa	ire				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SDXR- 061021/2197
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SDXR- 061021/2198
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SDXR- 061021/2199
sdxr2_5g_firm	iware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SDXR- 061021/2200
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descrip	tion & CVE	ID	Pa	tch	NCI	IPC ID
			Snapdragon	Wearable	es .				
			CVE ID : CV	E-2021-1	939				
Use After Free	17-Sep-21	10	to improper device addr frame in Sna Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Snapdragon Infrastructu	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976				_	A-SDXR- 21/2201
			CVE ID : CV	E-2021-1	976				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261			•	comm. ompan luct- cy/bull august	_	A-SDXR- 21/2202
sd_455_firmw	are								
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		0-QUA-SD_4- 061021/2203		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1976		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD_4- 061021/2204
			CVE ID : CVE-2021-30261		
sd_636_firmw	are				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SD_6- 061021/2205
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	O-QUA-SD_6- 061021/2206

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	-2021- bulletin	
sd_675_firmw	are				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD_6- 061021/2207
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SD_6- 061021/2208
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://ww w.qualcomm. com/compan y/product- security/bull	O-QUA-SD_6- 061021/2209

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
sd_8cx_firmw	are		from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	etins/august -2021- bulletin			
Su_ocx_III III w			Descible integer and hear	<u> </u>			
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SD_8- 061021/2210		
sd_8c_firmwa	re						
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SD_8- 061021/2211		
sm4125_firmware							
sm4125_firm	ware						

Weakness	Publish Date	CVSS	D	escriptio	n & CVE	ID	Pa	tch	NCI	IPC ID
Pointer Dereference			occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939			com/c y/prod securi	ty/bull august -	06102	21/2212	
Use After Free	17-Sep-21	7.2	kernel becaus pointer Compu Connec Industr Mobile Weara Wired Netwo	graphic se of stor r in Snap ite, Snap ctivity, S rial IOT, e, Snapdi bles, Sna Infrastr rking	apdrago ucture a	nvalid gon agon n	com/c y/prod securi	comm. compan duct- ty/bull august	_	A-SM41- 21/2213
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976			com/c y/prod securi	comm. compan duct- ty/bull august	_	A-SM41- 21/2214	
sm6250p_firr	1									
Use After	17-Sep-21	10			e can oc		https:/			A-SM62-
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Free			to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	061021/2215
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SM62- 061021/2216
sm6250_firm	ware			l	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SM62- 061021/2217

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Descript	ion & CVE	ID	Pa	tch	NCI	IPC ID	
			Networking							
			CVE ID : CVE	-2021-1	976					
Improper Input Validation	17-Sep-21	7.2	Possible integoverflow due command size while handling template upder from HLOS in Auto, Snapdra IOT, Snapdra Snapdragon I Snapdragon I Snapdragon I CVE ID: CVE	com/c y/prod securit	comm. ompan duct- ty/bull august		A-SM62- 21/2218			
sm7250_firmware										
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables			https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		_	A-SM72- 21/2219	
			CVE ID : CVE							
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			com/c y/prod securit	comm. ompan duct- ty/bull august	_	A-SM72- 21/2220	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1947		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA-SM72- 061021/2221
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA-SM72- 061021/2222
sm7325_firm	ware				
NULL		4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA-SM73- 061021/2223
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID: CVE-2021-1939		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM73- 061021/2224
wcd9306_firn	nware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA- WCD9- 061021/2225
wcd9326_firn	nware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	O-QUA- WCD9- 061021/2226
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	bulletin	
wcd9330_firm	nware				
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA- WCD9- 061021/2227
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCD9- 061021/2228
wcd9335_firm	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature	https://ww w.qualcomm. com/compan y/product-	O-QUA- WCD9- 061021/2229

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

1-2

0-1

CVSS Scoring Scale

		Description & CVE ID	Patch	NCIIPC ID
		enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	security/bull etins/august -2021- bulletin	
17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WCD9- 061021/2230
		CVE ID : CVE-2021-1947		
iware				
17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVF ID: CVF-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WCD9- 061021/2231
		Use-after-free vulnerability in	https://ww	
17-Sep-21	7.2	kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	w.qualcomm. com/compan y/product- security/bull etins/august	0-QUA- WCD9- 061021/2232
	ware 17-Sep-21	17-Sep-21 4.9 17-Sep-21 7.2	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Compute, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947  Ware  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947  Ware  Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Comyoute, Snapdragon Compute, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Wearables CVE ID: CVE-2021-1939  Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947	-2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WCD9- 061021/2233
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCD9- 061021/2234
wcd9341_firm	nware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon	https://ww w.qualcomm. com/compan y/product- security/bull	O-QUA- WCD9- 061021/2235
CVSS Scoring Sca	ile <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947		
wcd9360_firi	nware				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WCD9- 061021/2236
wcd9370_firm	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WCD9- 061021/2237
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon	https://ww w.qualcomm. com/compan y/product-	O-QUA- WCD9- 061021/2238

2-3 3-4 4-5

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	cvss	Desc	ription & CVI	ID	Pa	tch	NCI	PC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947			securit etins/a -2021- bulleti	august		
Use After Free	17-Sep-21	10	to improp device add frame in S Snapdrage Snapdrage Snapdrage Snapdrage Snapdrage Snapdrage Snapdrage Snapdrage Infrastruc Networkin	ture and	n of P2P Request Auto, vity, er IOT, al IOT, Music, es,	com/c	comm. ompan luct- cy/bull nugust	0-QUA WCD9 06102	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			_	comm. ompan luct- cy/bull nugust	0-QUA WCD9 06102	
wcd9371_firm	nware								
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the			_	//ww comm. ompan	0-QUA WCD9 06102	
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3	-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	y/product- security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA- WCD9- 061021/2242
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCD9- 061021/2243
wcd9375_firm			Null pointer dereference	https://ww	O-QUA-
Pointer	17-Sep-21	4.9	occurs due to improper	w.qualcomm.	WCD9-
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

		CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	com/compan y/product- security/bull etins/august -2021- bulletin	061021/2244
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCD9- 061021/2245
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WCD9- 061021/2246
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://ww w.qualcomm. com/compan	O-QUA- WCD9- 061021/2247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	y/product- security/bull etins/august -2021- bulletin	
wcd9380_firm	nware			1	
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCD9- 061021/2248
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCD9- 061021/2249
Use After Free  CVSS Scoring Sca	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,  2-3 3-4 4-5 5-6	https://www.qualcomm.com/company/product-	0-QUA- WCD9- 061021/2250

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCD9- 061021/2251
wcd9385_firm	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCD9- 061021/2252
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid	n https://ww w.qualcomm. com/compan	0-QUA- WCD9- 061021/2253
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947	y/product- security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCD9- 061021/2254
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCD9- 061021/2255
wcn3610_firn	nware		N. II	1	0.0114
NULL Pointer	17-Sep-21	4.9	Null pointer dereference occurs due to improper	https://ww w.qualcomm.	O-QUA- WCN3-
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 <b>9-10</b>

Dereference			validation when the	com/compan	0.64.004./0055
			preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	y/product- security/bull etins/august -2021- bulletin	061021/2256
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2257
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2258
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://ww w.qualcomm. com/compan	O-QUA- WCN3- 061021/2259

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	y/product- security/bull etins/august -2021- bulletin	
wcn3615_firm	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCN3- 061021/2260
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2261
Use After Free  CVSS Scoring Sca	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto,  2-3 3-4 4-5 5-6	https://ww w.qualcomm. com/compan y/product-	O-QUA- WCN3- 061021/2262

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1976	security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan	O-QUA- WCN3- 061021/2263
wcn3620_firm	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCN3- 061021/2264
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability is kernel graphics driver because of storing an invalid	w.qualcomm.	O-QUA- WCN3- 061021/2265
CVSS Scoring Sca	ale 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947	y/product- security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2266
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2267
wcn3660b_fir	mware		Null naintay dayafayanga	https://www	0.0114
NULL Pointer	17-Sep-21	4.9	Null pointer dereference occurs due to improper	https://ww w.qualcomm.	O-QUA- WCN3-
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Dereference			Description & CVE ID	Patch	NCIIPC ID
Deference			validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	com/compan y/product- security/bull etins/august -2021- bulletin	061021/2268
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2269
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2270
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation	https://ww w.qualcomm. com/compan	O-QUA- WCN3- 061021/2271

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	y/product- security/bull etins/august -2021- bulletin	
wcn3660_firm	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2272
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2273
Improper Input	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input	https://ww w.qualcomm.	O-QUA- WCN3-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Validation			command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	com/compan y/product- security/bull etins/august -2021- bulletin	061021/2274
wcn3680b_fir	mware		Ly n	T	
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2275
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2276
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request	https://ww w.qualcomm. com/compan	O-QUA- WCN3- 061021/2277
CVSS Scoring Sca	ile 0-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	y/product- security/bull etins/august -2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCN3- 061021/2278
wcn3680_firm	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables  CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2279
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P	https://ww w.qualcomm.	O-QUA- WCN3-
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			device address in PD Requestrame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	ct com/compan y/product- security/bull etins/august -2021- bulletin	061021/2280
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan	O-QUA- WCN3- 061021/2281
wcn3910_firn	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCN3- 061021/2282
Use After	17-Sep-21	7.2	Use-after-free vulnerability i	n https://ww	O-QUA-
CVSS Scoring Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6</b>	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
Free			kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1947	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	WCN3- 061021/2283			
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCN3- 061021/2284			
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCN3- 061021/2285			
wcn3950_firn	wcn3950_firmware							
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3 3-4 4-5 5-6 Page 8/11 of 8/61	6-7 7-8	8-9 9-10			

			NY 11 1 . C		
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA- WCN3- 061021/2286
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WCN3- 061021/2287
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WCN3- 061021/2288
Improper	17-Sep-21	7.2	Possible integer and heap	https://ww	O-QUA-

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Input Validation			overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	WCN3- 061021/2289
wcn3980_firm	nware				
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WCN3- 061021/2290
wcn3988_firm	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WCN3- 061021/2291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2292
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCN3- 061021/2293
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2294

2-3 3-4 4-5

CVSS Scoring Scale

0-1

5-6

6-7

7-8

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID					
wcn3990_firm	nware									
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA- WCN3- 061021/2295					
wcn3991_firmware										
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2296					
Use After Free	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947		https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2297						

2-3 3-4 4-5

5-6

6-7

8-9

7-8

CVSS Scoring Scale

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2298
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2299
wcn3998_firn	nware				l
NULL Pointer Dereference	NULL Pointer 17-Sep-21 4.9 Sna Sna Sna Sna		Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2300
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1939		
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2301
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2302
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN3- 061021/2303

5-6

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	CVSS	ı	Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			CVE II	D : CVE-	2021-30	)261				
wcn3999_firn	nware									
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976				_	comm. ompan luct- cy/bull august	0-QUA WCN3 06102	
			CVE II	<b>D</b> : <b>CVE</b> -2	2021-19	976				
wcn6740_firn	nware									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables				_	comm. ompan luct- cy/bull august	0-QUA WCN6 06102	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables,			https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin		O-QUA- WCN6- 061021/2306		
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	De	escriptio	on & CVE	ID	Pa	tch	NCI	IPC ID
			Snapdra Infrastr Networ	ucture						
			CVE ID	: CVE-2	2021-19	976				
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261				_	comm. ompan luct- cy/bull nugust	0-QUA WCN6 06102	
wcn6750_firn	nware									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939				_	comm. ompan luct- cy/bull nugust	0-QUA WCN6 06102	
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music,				com/com/com/com/com/com/com/com/com/com/	comm. ompan luct- cy/bull nugust	0-QUA WCN6 06102	
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description	n & CVE ID		Pat	ch	NCI	IPC ID
			Snapdragon W Snapdragon W Infrastructure Networking	'ired					
			CVE ID : CVE-2	2021-1976	•				
Improper Input Validation	17-Sep-21	7.2	template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		https://w.quald.com/com/com/com/com/com/com/com/com/com/	comm. ompan uct- y/bull ugust	0-QUA WCN6 06102		
			CVE ID : CVE-2	2021-3026	51				
wcn6850_firn	nware								
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer de occurs due to i validation whe preemption fer enablement is Snapdragon Au Snapdragon Co Snapdragon Co Snapdragon Co Snapdragon US Snapdragon W CVE ID : CVE-2	https://w.qualdcom/com/co y/prod security etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	0-QUA WCN6 06102			
Use After Free	17-Sep-21	7.2	Use-after-free kernel graphic because of stor pointer in Snap Compute, Snap Connectivity, S Industrial IOT, Mobile, Snapdr	https://w.quald.com/co y/prod security etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	0-QUA WCN6 06102			
CVSS Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking		
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2F device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	•	O-QUA- WCN6- 061021/2313
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCN6- 061021/2314
wcn6851_firm	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021-	O-QUA- WCN6- 061021/2315
CVSS Scoring Sca	ale <b>0-1</b>	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN6- 061021/2316
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA- WCN6- 061021/2317
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Industrial	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN6- 061021/2318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261				
wcn6855_firm	nware						
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN6- 061021/2319		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WCN6- 061021/2320		
wcn6856_firmware							
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto,	https://ww w.qualcomm. com/compan y/product- security/bull etins/august	O-QUA- WCN6- 061021/2321		

**2-3 3-4 4-5** 

1-2

0-1

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & C	/E ID	Patch	1	NCI	IPC ID
			Snapdragon Compu Snapdragon Connec Snapdragon Consun Snapdragon Industr Snapdragon Wearal CVE ID: CVE-2021	-2021- bulletin				
Use After Free	17-Sep-21	10	A use after free can to improper validate device address in PI frame in Snapdrago Snapdragon Compu Snapdragon Connect Snapdragon Consum Snapdragon Industric Snapdragon Wearalt Snapdragon Wearalt Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021	https://w.qualco com/com y/produ security/ etins/au -2021- bulletin	omm. npan ct- /bull	0-QUA WCN6 06102		
Improper Input Validation	17-Sep-21	7.2	Possible integer and overflow due to lack command size valid while handling bead template update confrom HLOS in Snaped Auto, Snapdragon Interpretation of Snapdragon Mobile, Snapdragon Wearald CVE ID: CVE-2021	https://w.qualco com/com/ y/produ security/ etins/au -2021- bulletin	omm. npan ct- /bull	0-QUA WCN6 06102		
whs9410_firm	nware							
Improper Input Validation	17-Sep-21	7.2	Possible integer and overflow due to lack command size valid while handling beach template update con	https://w w.qualco com/com y/produ security/	mm. npan ct-	0-QUA WHS9 06102		
CVSS Scoring Sca	ile 0-1	1-2	<b>2-3</b> 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	etins/august -2021- bulletin	
wsa8810_firm	nware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WSA8- 061021/2325
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WSA8- 061021/2326
Use After Free  CVSS Scoring Sca	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,  2-3 3-4 4-5 5-6	https://www.qualcomm.com/company/product-security/bulletins/august	0-QUA- WSA8- 061021/2327

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	-2021- bulletin	
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WSA8- 061021/2328
wsa8815_firm	iware				
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	0-QUA- WSA8- 061021/2329
Use After Free  CVSS Scoring Sca	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bull	0-QUA- WSA8- 061021/2330

Weakness	Publish Date	cvss		Description	on & CVE	ID	Pat	tch	NCI	IPC ID
			Indust Mobile Weara Wired Netwo	rial IOT e, Snapd bles, Sn Infrastr rking	Snapdra , Snapdr ragon apdrago ructure a	ragon on and	etins/a -2021- bulleti			
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976			_	comm. compan luct- y/bull nugust	0-QUA WSA8 06102		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables  CVE ID: CVE-2021-30261			https:/ w.qual com/co y/prod securit etins/a -2021- bulletin	comm. compan luct- y/bull nugust	0-QUA WSA8 06102		
wsa8830_firm	nware									
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature			https:/ w.qual com/co y/prod	comm.	0-QUA WSA8 06102		
CVSS Scoring Sca	ale <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	security/bull etins/august -2021- bulletin	
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	O-QUA- WSA8- 061021/2334
Use After Free	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WSA8- 061021/2335
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command	https://ww w.qualcomm. com/compan y/product- security/bull	O-QUA- WSA8- 061021/2336

5-6

6-7

7-8

8-9

9-10

**2-3 3-4 4-5** 

CVSS Scoring Scale

Weakness	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID: CVE-2021-30261	etins/august -2021- bulletin	
wsa8835_firm	ıware				,
NULL Pointer Dereference	17-Sep-21	4.9	Null pointer dereference occurs due to improper validation when the preemption feature enablement is toggled in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables CVE ID: CVE-2021-1939	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WSA8- 061021/2337
Use After Free	17-Sep-21	7.2	Use-after-free vulnerability in kernel graphics driver because of storing an invalid pointer in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1947	https://ww w.qualcomm. com/compan y/product- security/bull etins/august -2021- bulletin	0-QUA- WSA8- 061021/2338
Use After Free  CVSS Scoring Sca	17-Sep-21	10	A use after free can occur due to improper validation of P2P device address in PD Request frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,  2-3 3-4 4-5 5-6	https://www.qualcomm.com/company/product-security/bulletins/august	0-QUA- WSA8- 061021/2339

Weakness	Publish Date	cvss	Descript	on & CVE	ID	Pat	ch	NC	IPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking  CVE ID: CVE-2021-1976			-2021- bulletin	n		
Improper Input Validation	17-Sep-21	7.2	Possible integer and heap overflow due to lack of input command size validation while handling beacon template update command from HLOS in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables  CVE ID: CVE-2021-30261			https:/ w.qualcom/co y/prod securit etins/a -2021- bulletin	comm. ompan uct- y/bull ugust	0-QUA WSA8 06102	
Zyxel									
zywall_vpn2s	_firmware								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Sep-21	5	A directory traversal vulnerability in the web server of the Zyxel VPN2S firmware version 1.12 could allow a remote attacker to gain access to sensitive information.  CVE ID: CVE-2021-35027			https://ww w.zyxel.com/ support/Zyx el_security_a dvisory_for_d irectory_trav ersal_and_co mmand_injec tion_vulnera bilities_of_VP N2S_Firewall .shtml			Z-ZYWA- 21/2341
Improper Neutralizatio n of Special Elements	29-Sep-21	7.2	A command injection vulnerability in the CGI program of the Zyxel VPN2S firmware version 1.12 could			https://ww w.zyxel.com/ support/Zyx el_security_a			Z-ZYWA- 21/2342
CVSS Scoring Sca	le <b>0-1</b>	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
		allow an authenticated, local	dvisory_for_d	
		user to execute arbitrary OS	irectory_trav	
		commands.	ersal_and_co	
		CVE ID : CVE-2021-35028	mmand_injec	
		0.11.0.1	tion_vulnera	
			bilities_of_VP	
			N2S_Firewall	
			.shtml	
	Publish Date	Publish Date CVSS	allow an authenticated, local user to execute arbitrary OS	allow an authenticated, local user to execute arbitrary OS commands.  CVE ID: CVE-2021-35028  CVE ID: CVE-2021-35028  CVE ID: CVE-2021-35028  CVE ID: CVE-2021-35028  CVE ID: CVE-2021-35028